LR krašto apsaugos ministerijai 2018-09-24 Nr. 20180924/03
kam@kam.lt

DĖL LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJOS PASIŪLYMŲ, SUSIJUSIŲ SU SAUGIOJO TINKLO DUOMENŲ CENTRO PASLAUGŲ REGLAMENTAVIMU (ĮSTATYMO PROJEKTO NR. 18-9700(2))

(1) Šiuo raštu asociacija „INFOBALT“ („**Infobalt“**) nori atkreipti dėmesį į konkurencijos iškraipymus IRT paslaugų rinkoje, kuriuos siūlo sukurti Lietuvos Respublikos krašto apsaugos ministerija (toliau – **KAM**), bei paprašyti susilaikyti nuo tokių ketinimų, kaip neteisėtų, nekuriančių jokios pridėtinės vertės užtikrinant valstybės informacinių išteklių saugumą ir nepagrįstai didinančių valstybės išlaidas.

I. FAKTINĖ SITUACIJA IR PAGRINDINIAI INFOBALT SIŪLYMAI

(2) 2018-08-20 KAM įregistravo *Valstybės informacinių išteklių valdymo įstatymo pakeitimo* projektą (projekto numeris 18-9700) (toliau – „**Įstatymo projektas**“). Įstatymo projektu siūloma pakeisti įstatymo nuostatas, kuriomis įtvirtinamas valstybės institucijoms reikiamų duomenų centrų paslaugų bei SVDPT („Saugiojo tinklo“) teisinius monopolius įstatymo lygmens teisės aktuose.

(3) Infobalt šiam Įstatymo projektui nepritaria. Infobalt pozicija dėl Įstatymo projekto neteisėtumo ir netikslingumo kartu su konkrečiais pasiūlymais buvo pateikti KAM 2018-09-07 (pridedama).

(4) Įvertinusi Infobalt ir kitų institucijų pateiktas pastabas KAM įregistravo atnaujintą įstatymo projektą (projekto numeris 18-9700(2)) (toliau – **Atnaujintas įstatymo projektas**). Nepaisant labai konkrečių Infobalt pateiktų pasiūlymų Atnaujintame įstatymo projekte buvo atsižvelgta tik į vieną Infobalt pastabą dėl to, kad Saugusis tinklas neturėtų priklausyti valstybei nuosavybės teise. Visos kitos Infobalt pastabos ir pasiūlymai buvo ignoruoti. Maža to, Atnaujinto įstatymo projekto nuostatomis siūloma išplėsti KAM kontroliuojamos biudžetinės įstaigos monopoliją dar plačiau, nei buvo numatyta pirminiame Įstatymo projekte.

(5) Analizuojant KAM įregistruoto Atnaujinto įstatymo projekto nuostatas tampa akivaizdu, kad įstatymu siūloma suteikti KAM teisę teikti praktiškai bet kokias IRT paslaugas, bet kuriems KAM nurodytiems subjektams. Savo ruožtu sprendimo teisė, dėl to kam bus teikiamos paslaugos, kokios paslaugos bus teikiamos ir kokia apimtimi jos bus teikiamos priklauso išimtinai nuo KAM diskrecijos, KAM saugomiems subjektams nepaliekant netgi galimybės spręsti, ar jiems KAM siūlomų paslaugų reikia.

(6) Toks reguliavimas nėra niekaip suderinamas su Lietuvos Respublikos Konstitucija, kurie leidžia riboti konstitucines teises tik įstatymo pagrindu, tik įstatymuose numatyta apimtimi ir tik tada, kai tokie ribojimai yra proporcingi. Toks reguliavimas nesukuria jokios pridėtinės vertės kuriant didesnį valstybės informacinių išteklių saugumą. Tuo tarpu monopolijų veikimą aiškinantys fundamentalūs ekonomikos dėsniai pakankamai aiškiai sako, kad monopolinėmis sąlygomis veikiančios biudžetinės įstaigos veikimas yra kuo tiesiausias kelias į valstybės išlaidų (kainų) didėjimą ir kokybės (įskaitant saugumo) mažėjimą. Šį

Asociacija INFOBALT
Mokslininkų g. 2A-128, 08412 Vilnius
Interneto svetainė http://www.infobalt.lt
Tel. (8-5) 262 26 23
El. paštas office@infobalt.lt
A.s. LT277300010155447502
AB „Swedbank“
Banko kodas 73000

fundamentalų ekonomikos dėsnį lemia žmogaus prigimtis, todėl jis galioja nepriklausomai nuo to, kokius gerus ketinimus turėtų tokios monopolijos valdytojas.

(7) Infobalt visiškai pritaria ir palaiko valstybės siekį užtikrinti didesnį informacinių išteklių saugumą. Visgi, Infobalt nėra suprantama, kodėl tokių tikslų turėtų būti siekiama neteisėtomis priemonėmis, dėl kurių neveiksmingumo (didėjančių kainų ir mažėjančios kokybės) jau yra žinoma iš anksto. Juo labiau, kad egzistuoja visiškai racionalios alternatyvos leidžiančios pasiekti tuos pačius tikslus alternatyviomis priemonėmis.

(8) Atitinkamai, žemiau Infobalt dar kartą pakartoja savo siūlomo modelio pagrindinius principus, kurie buvo išdėstyti 2018-09-07 KAM adresuotame rašte. Kartu Infobalt išreiškia kritiką Atnaujintame įstatymo projekte atsiradusiems papildomiems ūkinės veiklos laisvės ribojimas.

II. INFOBALT SIŪLYMAS DĖL VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ APSAUGOS

(9) Infobalt siūlomas Saugaus tinklo modelis grindžiamas žemiau nurodytais principais, kurie buvo išsamiai paaiškinti 2018-09-07 KAM adresuotame rašte:

(i) **Siekiant užtikrinti saugumą nebūtina pačiam teikti visas IRT paslaugas – valstybė gali pasiekti pageidaujamą saugumo lygmenį formuluodama kokybinius reikalavimus valstybės institucijų perkamoms IRT paslaugoms ir veikdama kaip kompetencijų centras**. Šiuo tikslu valstybė gali nustatyti reikalavimus tinklo paslaugoms ir padėti valstybės institucijoms įsigyti tokias paslaugas (pvz. per standartinių pirkimo dokumentų rengimą, konsultacijas vykdant viešojo pirkimo procedūras ar net viešojo pirkimų procedūrų atlikimą pagal perkančiosios organizacijos išduotą įgaliojimą ir t.t.).

(ii) **Siekiant išgauti konsoliduotų IRT paslaugų pirkimo ekonominį efektą (t.y. kainų sumažėjimą perkant didesnius kiekius paslaugų) nėra būtina pačiam pirkti ir perparduoti paslaugas.** Veikdama kaip kompetencijų centras KAM kontroliuojama biudžetinė įstaiga gali apjungti norimą skaičių pirkimų mažiausiai dviem Viešųjų pirkimų įstatyme numatytais būdais: veikdama kaip centrinė perkančioji organizacija arba vykdydama pirkimus pagal atskirų valstybės institucijų išduotus standartinius įgaliojimus.

(iii) **Siekiant gauti geriausios kokybės paslaugas būtina užtikrinti tiekėjų konkurenciją.** Tik konkurencijos sąlygomis tiekėjai yra skatinami mažinti savo paslaugų kainas, didinti efektyvumą ir diegti naujas inovatyvias technologijas. Valstybei nustatant techninius reikalavimus, o Saugiojo tinklo valdytojui padedant parinkti tiekėjus ir kontroliuojant jų teikiamų paslaugų kokybę (atliekant auditus, patikrinimus ir t.t.) tiekėjai gali konkuruoti tarpusavyje siūlydami efektyviausias ir mažiausiai sąnaudų reikalaujančias technologijas tokiems tikslams pasiekti. Tai nereiškia, kad Saugiojo tinklo paslaugas gali teikti nepatikimi subjektai. Infobalt sutinka su tuo, kad valstybė gali nustatyti specialius saugumo reikalavimus tiekėjams ir/ar reikalauti nutraukti sutartis su nepatikimais tiekėjais t.t. Tačiau Infobalt griežtai nesutinka su tuo, kad tik monopolijos sukūrimas leidžia apsisaugoti nuo nepatikimų tiekėjų.

(iv) **Saugusis tinklas turi būti naudojamas tik ribotų darbo vietų atžvilgiu.** Saugusis tinklas yra saugus tiek, kiek yra saugi tinklo silpniausia vieta. Valstybė neturi tiek lėšų, kad kiekvienos valstybės ir savivaldybių kontroliuojamų subjektų darbo vietos atžvilgiu valstybė galėtų įdiegti sudėtingus techninius saugumo sprendimus. Todėl nepagrįstai išplėtus Saugiojo tinklo paslaugų apimtį, susiformuos silpnosios (mažiau apsaugotos) tinklo grandys, kurios galės tapti vartais į visą Saugųjį tinklą. Dėl šios priežasties, Saugusis tinklas turėtų būti naudojamas tik tų darbų vietų atžvilgiu, kurios valdo saugomą informaciją ar turi tokią prieigą prie saugomų informacinių išteklių, kuri suteikia galimybę keisti saugomų duomenų turinį. Apribojusi Saugiojo tinklo apimtį

iki tokių objektų, kuriems realiai reikia didesnės apsaugos, valstybė galėtų skirti adekvatų dėmesį ir lėšų tokių objektų apsaugai, tokiu būdu išvengiant silpnųjų tinklo vietų susiformavimo.

(v) Apskritai, Infobalt nėra suprantama kaip KAM kontroliuojama biudžetinė įstaiga sugebės kokybiškai suteikti Saugiojo tinklo paslaugas tokios apimties darbo vietų atžvilgiu. Atnaujintame įstatymo projekte Saugiojo tinklo naudotojams *de facto* gali būti priskirtos bet kokios valstybės ir savivaldybės institucijos ir įstaigos, valstybės įmonės ir viešosios įstaigos. Tai yra tūkstančiai darbo vietų ir informacinių išteklių, kurie neturi nieko bendro su saugomais valstybės informaciniais ištekliais. Saugant tokios apimties subjektus, kurie turi labai netolygius saugumo poreikius, tinklo saugumas bus neišvengiamai pažeistas.

(vi) **KAM gali vykdyti Saugiojo tinklo valdymą, nepriklausomai nuo to, kad Saugiojo tinklo paslaugas teikia privatūs rinkos dalyviai.** KAM siūlomas modelis panašu yra grindžiamas KAM tikslu užsitikrinti Saugiojo tinklo valdymą, t.y. galimybe suvaldyti krizinę situaciją priimant ir įgyvendinant reikiamus tinklo sprendimus. Infobalt atkreipia dėmesį, kad tinklo valdymo teisių suteikimas KAM yra tik vienas iš daugelio kokybinių kriterijų Saugiajam tinklui, kuriuos gali nustatyti valstybė. Visgi valdyti tinklą KAM gali ir tuo atveju, jeigu Saugiojo tinklo paslaugas teikia privatūs rinkos dalyviai. Nėra būtina monopolizuoti paslaugos tam, kad KAM turėtų tinklo valdymo teises.

(vii) **KAM gali teikti paslaugas, kurių nenori ar negali teikti privatūs subjektai.** Infobalt sutinka su tuo, kad atskirų subjektų ar saugomų valstybės informacinių išteklių atžvilgiu KAM gali turėti poreikį naudoti technologijas, kurios nėra prieinamos privatiems rinkos dalyviams (t.y. rinka tokių paslaugų suteikti negali). Infobalt sutinka, kad tokias specifines paslaugas (kurių negali pasiūlyti rinką) KAM galėtų teikti. Tokių paslaugų teikimas būtų suderinamas su Konstitucijos ir Europos Sąjungos teisės nuostatomis.

(viii) **Saugiojo tinklo veikimas turi užtikrinti „keturių akių" principą.** Privatiems rinkos dalyviams teikiant Saugiojo tinklo paslaugas pagal valstybės nustatytus kriterijus, o paslaugų teikimo kokybę kontroliuojant Saugiojo tinklo tvarkytojui būtų užtikrinamas „keturių akių" principas. Nesunku numanyti, kad KAM veikiant kaip Saugiojo tinklo paslaugų teikėjui ir tuo pačiu kontroliuojant savo teikiamų paslaugų kokybę, *de facto* niekas kokybės nevertins ir neužtikrins, o kitos valstybės institucijos tikrosios padėties apie Lietuvos kibernetinį saugumą niekada nežinos iki didesnių kibernetinių incidentų.

(10) Mūsų nuomone, įgyvendinus aukščiau nurodytus principus būtų pasiekti visi KAM siekiami tikslai, nesukuriant konkurencijos iškraipymų ir neišvengiamo valstybės išlaidų didėjimo, kurį garantuoja KAM biudžetinės įstaigos veikimas monopolinėmis sąlygomis be jokio kontrolės mechanizmo. Todėl siūlytume juos pakartotinai įvertinti ir apsvarstyti.

III. ATNAUJINTO PROJEKTO KRITIKA

(11) Infobalt labai nustebino KAM įregistruotas Atnaujintas įstatymo projektas. Nors Infobalt teikė labai konstruktyvius pasiūlymus, kaip įmanoma užtikrinti kibernetinį saugumą bendradarbiaujant valstybei ir verslui, Atnaujintame įstatymo projekte siūloma numatyti dar platesnės apimties monopoliją. Infobalt nuomone, šis projektas negali būti priimtas mažiausiai dėl kelių priežasčių.

(12) ***Pirma***, Atnaujintame įstatymo projekte naujai numatoma, kad Saugiojo tinklo paslaugos *privalomai* bus teikiamos ne tik institucijoms, tačiau ir valstybės įmonėms bei viešosioms įstaigoms. Toks išplėtimas kritikuotinas bent keliais aspektais. Infobalt abejoja ar visos Lietuvos valstybės ir savivaldybės kontroliuojamiems subjektams paslaugas teikianti KAM sugebės (jeigu sugebės, tai kada) suteikti paslaugas, kuriuos užtikrintų tokių skirtingų subjektų poreikius. Tai ypač taikoma strateginėms valstybės įmonėms, kuriuos jau dabar turi įdiegusios jų poreikius atitinkančias, aukšto lygio kibernetinės saugos

priemones, kurių turės būti atsisakoma nepaisant padarytų investicijų vien dėl to, kad KAM kontroliuojama biudžetinė įstaiga galėtų suteikti savo *standartines* paslaugas. Infobalt apskritai nesuprantama kodėl KAM – karinė struktūra – turi saugoti visos Lietuvos informacinius išteklius pati teikdama paslaugas. Tokios apimties paslaugų suteikti kokybiškai, atsiliepiant į paslaugos gavėjų interesus, užtikrinant reikiamus reakcijos laikus yra neįmanoma, ypač kai paslaugų pirkėjui atimama teisė nepirkti KAM biudžetinės įstaigos paslaugų.

(13) ***Antra***, pirminis įstatymo projektas grindė Saugiojo tinklo paslaugų teikimą neva egzistuojančiu poreikiu vykdyti mobilizacines užduotis (kurios lėmė ir Saugiojo tinklo naudotojų apimtį), Atnaujintas įstatymo projektas siūlo numatyti galimybę papildomai išplėsti monopoliją iki visų institucijų turinčių „*gyvybiškai svarbias valstybės funkcijas*“. Kadangi gyvybiškai svarbių valstybės funkcijų sąrašas neegzistuoja, o tam tikra prasme bet kuri valstybės funkcija yra gyvybiškai svarbi, toks monopolijos išplėtimas *de facto* reiškia, kad KAM gali nuspręsti teikti Saugiojo tinklo paslaugas bet kuriam subjektui, dėl kurio KAM priims atitinkamą sprendimą. Įstatymo projekte neegzistuoja jokių saugiklių, kurie leistų patikrinti ar KAM pagrįstai nusprendė įpareigoti atskirus subjektus naudotis Saugiojo tinklo paslaugomis.

(14) ***Trečia,*** Atnaujintas įstatymo projektas sukuria prielaidas reikšmingai didinti valstybės išlaidas IRT paslaugų įsigijimui, kadangi projekte nėra absoliučiai jokių saugiklių leidžiančių kontroliuoti KAM kontroliuojamos biudžetinės įstaigos sąnaudų ar paslaugų apimties. KAM siūlomame modelyje vienintelė institucija galinti spręsti dėl Saugaus tinklo naudojamos įrangos pobūdžio ir kiekio yra pati KAM kontroliuojama biudžetinė įstaiga. Saugiojo tinklo paslaugų gavėjui nėra svarbu kiek ir kokios įrangos jam bus įrengta, nes už tokią įrangą jis bet kokiu atveju nemokės (pvz. kodėl Paslaugų teikėjas turėtų prašyti sumažinti Saugiojo tinklo tvarkytojo aptarnaujamų darbų vietų skaičių, jeigu buvo panaikintas atitinkamas etatas). KAM neturės kompetencijos kontroliuoti Saugiojo tinklo tvarkytojo montuojamos įrangos pobūdžio ar kiekio, nes visos kompetencijos bus sutelktos Saugiojo tinklo tvarkytojo lygmenyje. Savo ruožtu, Saugioji tinklo tvarkytojas nebus suinteresuotas įrengti tik tiek ir tokios įrangos, kurios reikia norint užtikrinti saugumą, kadangi už šią įrangą bet kokiu atveju moka valstybės biudžetas, o didesnės ir sudėtingesnės įrangos naudojimas (net kai to objektyviai nereikia) tik parodo Saugiojo tinklo valdytojo didesnę reikšmę valstybėje. Įdomu ir tai, kad Finansų ministerija, Valstybės kontrolė ar bet kurios kitos institucijos negalės nieko pasakyti apie KAM kontroliuojamos biudžetinės įstaigos patiriamų sąnaudų racionalumą, kadangi visi sąnaudų pagrįstumą vertinti leidžiantys parametrai bus slapti ir nepalyginami su rinkoje prieinamomis alternatyvomis.

(15) ***Ketvirta,*** nors Atnaujinto įstatymo projekto 43^2 str. 5 ir 7 dalimis siekiama sudaryti iliuziją, kad Saugiojo tinklo paslaugų sąrašas yra ribotas įstatyme numatytu paslaugų sąrašu, analizuojant 5 dalyje įtvirtiną paslaugų sąrašą galima aiškiai matyti, kad Saugiojo tinklo valdytojas gali teikti bet kokias IRT pasaugas, kurias tik pageidauja. 43^2 str. 5 d. 1 ir 2 p. realiai sako, kad Saugaus tinklo tvarkytojas teiks rinkoje visiškai įprastas duomenų perdavimo paslaugas (Atnaujintas įstatymo projektas šiuo atveju papildomai numato, kad perdavimas bus užtikrinamas ne tik „tarp“ padalinių ir institucijų, bet padaliniams ir institucijoms). Savo ruožtu, 43^2 str. 5 d. 3 p. pateikta nuoroda į „kibernetinės saugumo priemones“ atveria KAM galimybę nuspręsti praktiškai dėl bet kokių paslaugų teikimo, nes praktiškai visos IRT paslaugos yra susijusios tiek su duomenų perdavimo ir apdorojimo paslaugomis, tiek su tokių paslaugų „kibernetiniu saugumu“. Kitaip tariant, Atnaujintas įstatymo projektas teigia, kad KAM galės viena pati nuspręsti tiek dėl to, kas turi pirkti paslaugas, tiek dėl to, kokios apimties paslaugas jie turės pirkti. Įstatymo projekte nėra jokio mechanizmo užtikrinančio, kad Saugiojo tinklo paslaugos apimtų tik tiek ir tokių paslaugų, kurių realiai reikia siekiant užtikrinti valstybės saugumą.

(16) ***Penkta***, Atnaujintas įstatymo projektas numato neefektyvius saugiklius kaštų didėjimui. 43^2 str. 8 d. numato, kad KAM biudžetinės įstaigos papildomų paslaugų teikimo kaštus tikrins audito įmonė, o įgaliota institucija vertins, ar papildomų paslaugų įkainiai buvo paskaičiuoti pagal nustatytus kriterijus. Mūsų nuomone, toks kontrolės mechanizmas sukurs tik kontrolės iliuziją. Auditoriai tikrina tik sąnaudų pagrįstumą ir paskirstymą, tačiau auditoriai nieko negali pasakyti apie tai, ar Saugiojo tinklo naudotojui buvo suteikta tik tiek ir tokių paslaugų, kurių realiai reikia norint užtikrinti saugumą. Auditoriai taip pat

negali nieko pasakyti apie tai, ar KAM paslaugų teikimo efektyvumas atitinka rinkoje įprastą efektyvumą (pvz. ar perkamos tinkamos technologijos, ar pagrįstos valdymo sąnaudos ir t.t.).

(17) ***Penkta,*** Atnaujintas įstatymo projektas nenumato absoliučiai jokių saugumo reikalavimų Saugiajam tinklui. Atnaujintas įstatymo projektas tiesiog sako, kad KAM teikia monopolines IRT paslaugas (sąlyginiu pavadinimu „Saugusis tinklas“), kurios neprivalo būti niekaip skirtingos nuo rinkoje privačių subjektų teikiamų paslaugų, tokios paslaugos neprivalo būti niekaip saugesnės. Saugumą garantuoja neva vien tas faktas, kad jas teikia KAM kontroliuojama biudžetinė įstaiga.

(18) ***Šešta,*** Aiškinamajame rašte KAM išdėstyta pozicija dėl Saugiojo tinklo paslaugų „nekomercinio pobūdžio“ (tai, kad tokių paslaugų monopolizavimas nėra laikomas ūkinės veiklos laisvės ribojimu) neturi jokio teisinio pagrindo. KAM referuoja į ESTT ir Komisijos praktiką selektyviai, nevertindama šių sprendimų faktinės ir teisinės situacijos skirtumų. Todėl Infobalt ir toliau laikosi ankstesniuose raštuose išdėstytos pozicijos, kad kuriant monopoliją yra pažeidžiamas Konstitucijos 46 str. bei Europos Sąjungos teisės nuostatos.

IV. PRAŠYMAS

(19) Apibendrinant, Infobalt prašo įvertinti išdėstytas pastabas ir iš esmės peržiūrėti Saugiojo tinklo organizavimo modelį pagal Infobalt pateiktus pasiūlymus, kuris leidžia pasiekti analogiškus tikslus efektyviau, skiriant mažesnius finansinius išteklius ir neribojant konkurencijos.

Priedai:

1. 2018-09-07 Infobalt raštas KAM.

INFOBALT direktorius [pasirašyta el. parašu] Paulius Vertelka

LR Krašto apsaugos ministerijai 2018-09-07 Nr. 20180907/01
kam@kam.lt

LR Vyriausybės kanceliarijai
LRVkanceliarija@lrv.lt

DĖL LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJOS PASIŪLYMŲ, SUSIJUSIŲ SU SAUGIOJO TINKLO IR DUOMENŲ CENTRO PASLAUGŲ REGLAMENTAVIMU (ĮSTATYMO PROJEKTO NR. 18-9700)

(1) Asociacija „INFOBALT“ („**Infobalt“**) yra nacionalinio informacinių ir ryšių technologijų sektoriaus asociacija. INFOBALT yra viena didžiausių asociacijų Lietuvoje. Įsikūrusi 1994 m. šiuo metu asociacija vienija daugiau kaip 170 Lietuvos informacinių ir ryšių technologijų įmonių bei mokslo ir studijų institucijų, kuriose dirba apie 10 000 informacinių ir ryšių technologijų specialistų.

(2) 2018-08-20 Lietuvos Respublikos krašto apsaugos ministerija (toliau – „Krašto apsaugos ministerija“ arba „KAM“) įregistravo *Valstybės informacinių išteklių valdymo įstatymo pakeitimo* projektą (projekto numeris 18-9700) (toliau – „**Įstatymo projektas**“). Įstatymo projektu siūloma pakeisti įstatymo nuostatas, kuriomis įtvirtinamas valstybės institucijoms reikiamų duomenų centrų paslaugų bei SVDPT („Saugiojo tinklo“) teisinius monopolius įstatymo lygmens teisės aktuose.

(3) Infobalt šiam Įstatymo projektui griežtai nepritaria. Mūsų nuomone, KAM siūlomos sukurti duomenų perdavimo paslaugų ir duomenų centrų paslaugų monopolijos (i) yra neteisėtos – pažeidžia Lietuvos Respublikos Konstituciją bei Europos Sąjungos teisės aktus; (ii) pakirs Lietuvos IT sektoriaus gyvybingumą; (iii) sieks užtikrinti duomenų saugumą metodais, kurie neatitinka geriausios NATO ir daugelio kitų šalių praktikos.

(4) Detalūs Infobalt argumentai šiais klausimais buvo išdėstyti 2018-06-18 KAM adresuotame rašte Nr. 20180618/01 „*Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 4, 5, 6, 22 ir 39 straipsnių pakeitimo ir įstatymo papildymo 43(2) ir 43(3) straipsniais įstatymo projekto“* (toliau – „**2018-06-18 raštas**“, Priedas Nr. 2). Kadangi šiame rašte kritikuojami analogiški KAM pasiūlymai kurti valstybines monopolijas, šių argumentų Infobalt nekartoja, tačiau 2018-06-18 raštą prideda prie šio rašto kaip priedą Nr. 2 ir prašo įvertinti 2018-06-18 rašte išdėstytas pastabas svarstant 2018-08-20 įregistruotą Įstatymo projektą (projekto numeris 18-9700).

(5) Savo ruožtu, šiame rašte Infobalt pateikia kritiką KAM pasiūlytam įstatymo projektui ir konstruktyvius pasiūlymus, kaip būtų galima pasiekti analogiškus tikslus efektyviau, skiriant mažesnius valstybės finansinius išteklius ir nenumatant nepagrįstų konkurencijos ribojimų.

I. PASIŪLYMAI SĄVOKAI „SAUGUSIS VALSTYBINIS DUOMENŲ CENTRAS (SAUGUSIS TINKLAS)“

(6) Įstatymo projekte siūloma įtvirtinti žemiau nurodytą Saugiojo tinklo sąvoką:

> *„13. Saugusis valstybinis duomenų perdavimo tinklas (toliau – Saugusis tinklas) – valstybei nuosavybės teise priklausantis, specialiuosius organizacinius ir techninius reikalavimus atitinkantis,*
> *nuo viešųjų elektroninių ryšių tinklų nepriklausomas, viešai neteikiamas elektroninių ryšių tinklas.“*

(7) Įstatymo projekte siūloma įtvirtinti Saugiojo tinklo sąvoka turi būti koreguojama bent keliais aspektais.

(i) ***Sąvokos elementas „valstybei nuosavybės teise priklausantis***“. Šis sąvokos elementas suponuoja, kad valstybė neišvengiamai privalo turėti nuosavybės teisę į tinklą ir kiekvieną tinklo elementą. Šis „nuosavybės“ reikalavimas taikomas netgi tada, kai analogiškas saugumas gali būti pasiekiamas nuomojantis infrastruktūrą ir/arba perkant infrastruktūros paslaugas, o naujos valstybinės infrastruktūros diegimas yra ekonomiškai neracionalus (brangesnis). Šis „valstybės nuosavybės“ aspektas ypatingai svarbus prijungiant prie Saugiojo tinklo nutolusius regionus – naujo fizinio tinklo tiesimas valstybės lėšomis *vien tik* kelių darbų vietų prijungimui visuomet bus labai brangus ir ekonomiškai niekaip nepasiteisinantis sprendimas. Maža to, atskirais atvejis jis nėra įgyvendinamas fiziškai / teisiškai. Pavyzdžiui, Lietuvos Respublikos diplomatinės ir konsulinės įstaigos užsienyje yra priskirtos Vyriausybės nutarimu Nr. 631[1] prie mobilizacines funkcijas vykdančių subjektų. Akivaizdu, kad nutiesti „valstybės nuosavybės teise“ priklausančio tinklo iki tokios atstovybės Briuselyje yra neįmanoma, o mažiausiai kitos šalies teritorijoje komunikacija turės būti vykdoma ir privatiems asmenims priklausančiais tinklais.

Kadangi nuosavybės teisės į kiekvieną Saugiojo tinklo elementą turėjimas automatiškai nesuponuoja didesnio tinklo saugumo, o tiesti naujų valstybinių tinklų tik tam, kad turėti nuosavybės teisę būtų neracionalu, siūlome šio sąvokos elemento atsisakyti ir palikti pareigą atsakingai institucijai nuspręsti kokiais konkrečiai techniniais sprendimais, kokiomis teisėmis į infrastruktūrą turėtų būti užtikrinamas tinklo saugumas.

(ii) ***„Nuo viešųjų elektroninių ryšių tinklų nepriklausomas“.*** Kaip nurodoma Įstatymo projekte ir KAM parengtame Įstatymo projekto aiškinamajame rašte (toliau – **Aiškinamasis raštas**), Saugusis tinklas nebus skirtas tik palaikyti vidinę komunikaciją tarp valstybės institucijų. Saugiuoju tinklu yra numatoma teikti „*nustatytos spartos prieigą prie viešųjų ryšių tinklų*“[2], kas iš principo reiškia, kad Saugusis tinklas turės sąsają su viešaisiais tinklais. Tai nurodoma ir Aiškinamajame rašte. Technine prasme tai reiškia, kad Saugusis tinklas nebus „nepriklausomas“ nuo viešųjų tinklų (kaip nurodoma Įstatymo projekte) – Saugusis tinklas tiesiog bus „apsaugotas“ nuo viešųjų tinklų naudojant specialiąsias priemones. Atitinkamai, Saugiojo tinklo sąvokoje siūlome atsisakyti teiginių apie tai, kad elektroninių ryšių tinklas turi būti „nepriklausomas“ nuo viešųjų elektroninių ryšių tinklų („nepriklausomumo“ terminas neturi jokio techninio paaiškinimo numatytame Saugiojo tinklo modelyje, todėl yra klaidinantis). Saugiojo tinklo apsaugojimas nuo viešųjų ryšių tinklų ir tokio apsaugojimo būdai yra santykinai paprastas techninis kibernetinės saugos apibūdinimas, todėl reikalavimą užtikrinti tinkamą apsaugą siūlome įtraukti į techninius reikalavimus Saugiajam tinklui, jų papildomai nedetalizuojant Saugiojo tinklo sąvokoje.

(iii) ***„Viešai neteikiamas elektroninių ryšių tinklas“.*** Sąvoka nėra tiksli. Nėra aišku, kur yra „viešai neteikiamo“ tinklo ribos, t.y. tik valstybės institucijos; tik valstybės institucijos ir valstybės kontroliuojamos įmonės; ar visos valstybės institucijos ir įmonės, ar tik institucijos ir įmonės valdančios jautrius duomenis ir t.t. Įstatymo projekte numatoma, kad Saugiuoju tinklu turės

[1] Lietuvos Respublikos Vyriausybės 2012 m. gegužės 29 d. nutarimas Nr. 631 „Dėl Gyvybiškai svarbių valstybės funkcijų sąrašo patvirtinimo“ (Žin., 2012, Nr. 64-3243)

[2] Įstatymo projekto 43[2] str. 3 d.

naudotis subjektai įrašyti į Saugiojo tinklo naudotojų sąrašą. Mūsų nuomone, tokia logika turėtų būti išlaikoma į „Saugiojo tinklo“ sąvokoje numatant, kad šiuo tinklu naudojasi *tik* institucijos esančios Saugiojo tinklo naudotojų sąraše.

Tai labai svarbu ir kibernetinio saugumo užtikrinimo klausimu. Suteikiant galimybę prie Saugiojo tinklo jungtis subjektams, kurie nevaldo jautrios informacijos ir neturi privilegijuotos prieigos prie informacinių išteklių ar valstybės registrų[3], Saugiajame tinkle susiformuos silpnosios grandys per kurias įsibrauti į tinklą bus gerokai lengviau piktų ketinimų turintiems subjektams. Siekiant užtikrinti tinklo saugumą prieiga prie Saugiojo tinklo turi būti ribota – tinklas turi būti prieinamas tik tokioms institucijoms ir tik tokia apimtimi, kiek tai yra būtina siekiant užtikrinti valstybei jautrios informacijos saugumą. Tik tokiu atveju tinkle įmanoma išlaikyti tolygų saugumo lygmenį. Tokiu principu veikia ir Europos Sąjungos TESTA tinklas – prieiga prie TESTA tinklo yra suteikiama tik pirmiausia įrodžius, kad konkrečioms institucijoms tokia prieiga yra objektyviai reikalinga ir tai, kad prieiga viešaisiais elektroniniais tinklais konkrečiu atveju nėra pakankama.

Atsižvelgiant į tai, siūlome keisti aiškių ribų nenustatantį sąvokos elementą „*viešai neteikiamas elektroninių ryšių tinklas*“ į tikslesnę ir su kitomis įstatymo projekto nuostatomis suderintą sąvoką „*elektroninių ryšių tinklas, kuriuo gali naudotis tik šio įstatymo nustatyta tvarka įvardinti Saugiojo tinklo naudotojai.*“

(8) **Apibendrinant**, Infobalt siūlo išdėstyti Saugiojo tinklo sąvoką taip:

„13. Saugusis valstybinis duomenų perdavimo tinklas (toliau – Saugusis tinklas) – krašto apsaugos ministro įgaliotos biudžetinės įstaigos valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis elektroninių ryšių tinklas, kuriuo gali naudotis tik šio įstatymo nustatyta tvarka įvardinti saugiojo tinklo naudotojai.“

II. RIBOTOS SAUGIOJO TINKLO PRIEIGOS PRINCIPAS

(9) Kaip suponuoja jau pati „Saugiojo tinklo“ sąvoka, šio tinklo įrengimas ir sprendimas skirti tinklo įrengimui papildomą valstybinį finansavimą yra grindžiamas poreikiu užtikrinti aukštesnio saugumo lygmens valstybės institucijų komunikaciją. Tai yra atsakingas valstybės sprendimas. Priimdama sprendimą, pakertantį privataus IT verslo vystymosi galimybes ir apribojantį Konstitucines teises, išleisti dideles papildomas lėšas naujos infrastruktūros kūrimui valstybė mažų mažiausiai turėtų tikėtis, kad kuriamas Saugusis tinklas garantuos apčiuopiamai didesnį kibernetinį saugumą.

(10) Dėl tų pačių priežasčių valstybei neturėtų būti priimtinas toks „Saugusis tinklas“, kuris taptų paprasčiausia privačių subjektų teikiamos viešojo elektroninių ryšių tinklo paslaugos alternatyva, kurio saugumą neva garantuoja vien tas faktas, kad visą tinklo infrastruktūrą valdo valstybės kontroliuojama įmonė. Be to, kad tokio naujo valstybinio paslaugų teikimo kūrimas neturi jokios prasmės, toks valstybinis subjektas niekuomet nesugebės pasiekti tokios paslaugų kokybės (įskaitant saugumo standartų), kurią rinkoje siūlo privatus verslas. Tai užtikrina fundamentalūs ekonomikos dėsniai, teigiantys, kad monopolijos sąlygomis tikėtis kokybės pagerėjimo ar kainos sumažėjimo neverta. Maža to, valstybinės – komercinės paslaugos vystymas nesukurs absoliučiai jokio papildomo kibernetinio saugumo valstybės institucijoms, ir priešingai – pareikalaus didelių valstybės investicijų ir pažeis Konstitucijos ir ES teisės aktų reikalavimus[4].

(11) Mūsų įsitikinimu, siekiant sukurti aukštesnės kibernetinės saugos tinklą, o ne standartinę rinkoje teikiamą paslaugą, pirmiausiai būtina riboti prieigą prie Saugiojo tinklo. Saugusis tinklas turi būti naudojamas (i)

[3] Teise įrašyti, pakeisti ar panaikinti duomenis.
[4] Apie tai plačiau žr. 2018-06-18 raštą.

tik tose įstaigose ir institucijose, kurios valdo informaciją, kurią reikėtų saugoti; ir (ii) tik toje šių subjektų veiklos apimtyje, kiek tokio tinklo naudojimas yra reikalingas norint užtikrinti aukštesnę kibernetinę saugą. Šis principas suponuoja mažiausiai tris sekmenis, kurie turėtų būti atspindėti įstatyme:

(i) Valstybė turi investuoti į „Saugaus tinklo“ kūrimą tik tose institucijose, kurios turi ką saugoti. Panašu, kad Įstatymo projekto rengėjai šį principą siūlo užtikrinti per „įrašymą“ į „Saugiojo tinklo naudotojų sąrašą“.

Su tokiu principu galima sutikti. Kita vertus, negalima sutikti su Įstatymo projektų rengėju pasiūlymu įtvirtinti, kad tokį sąrašą sudaro „*Vyriausybė arba jos įgaliota institucija*“. Pareiga naudoti „Saugųjį tinklą“ apriboja Konstitucines teises (Konstitucijos 46 str. numatytą draudimą monopolizuoti rinką bei riboti ūkinės veiklos laisvę). Pagal Konstitucinio teismo praktiką, bet kokie konstitucinių teisių ribojimai gali būti vykdomi tik įstatymo lygmens teisės aktais. Atitinkamai, siūlome įstatymo projektą koreguoti numatant, kad „*Saugiojo tinklo naudotojų sąrašas*“ tvirtinamas įstatymo lygmens teisės aktu.

(ii) Valstybė neturi investuoti į saugumo užtikrinimą tokiose darbo vietose, kurios naudojasi elektroninių ryšių tinklais taip, kaip tai darytų kiekvienas Lietuvos gyventojas ar privataus verslo darbuotojai, neturintys privilegijuotos prieigos prie jokios saugomos valstybės informacijos. Pavyzdžiui, valstybė turi poreikį investuoti į tokių darbo vietų apsaugą, kurioje saugoma valstybei jautri informacija, tačiau neturi poreikio investuoti į tokių darbo vietų apsaugą, kurių vienintelis tikslas turėti interneto ryšį komunikacijai su visuomene, informacijos paieškai ir t.t. Todėl siūlome įstatymo projekte numatyti „*Saugomos informacijos*“ sąvoką. Ši sąvoka apibrėžtų pirmąjį „Saugaus tinklo“ perimetro elementą – „Saugusis tinklas“ įrengiamas tik tose darbo vietose, kuriose yra „saugomos informacijos“;

(iii) Valstybė neturi investuoti į saugumo užtikrinimą tokiose darbo vietose, kurios jungiasi prie valstybės informacinių išteklių ir registrų, neturėdamos teisės šiuos ištekliuose esančių duomenų įvesti, pakeisti ar pašalinti. Jeigu šiuos išteklius gali pasiekti kiekvienas Lietuvos gyventojas, tokios prieigos saugumas yra užtikrinamas standartinėmis viešųjų išteklių prieigos apsaugos priemonėmis, „saugiojo tinklo“ naudojimas tokią prieigą turinčioms darbo vietoms nesukurs jokio papildomo saugumo valstybės informaciniams ištekliams / registrams. Todėl siūlome įstatymo projekte numatyti „*Privilegijuotos prieigos prie informacinių išteklių*“ sąvoką. Ši sąvoka apibrėžtų antrąjį „saugaus tinklo“ perimetro elementą – „Saugusis tinklas“ įrengiamas tik tose vietose, kurios turi teisę daryti įtaką tokiems ištekliams (atlikti išteklių ar sistemų funkcionavimo, palaikymo ar atstatymo veiksmus.

(12) Šiame kontekste atkreipiame dėmesį į kelis techninius „saugaus tinklo“ kūrimo aspektus.

(13) ***Pirma***, techniniu požiūriu įmanoma tinkamai apsaugoti duomenis *tos pačios įstaigos* lygmenyje, jeigu vienos darbo vietos naudojasi „Saugiuoju tinklu“, o kitos – rinkos teikiamomis įprastomis elektroninių ryšių paslaugomis. Šis klausimas yra išimtinai susijęs su Saugiojo tinklo perimetro nustatymu. Skirtumas tik tas, kad kibernetinio saugumo priemonės diegiamos ne įstaigos teritorijos ribose, tačiau įstaigos tinklų susijungimo riboje, esančioje toje pačioje įstaigoje. Atitinkamai, Infobalt teikiamas siūlymas yra išsprendžiamas techniškai ir būtų visiškai įprasta rinkos praktika.

(14) ***Antra,*** tik apribojus prieigą prie Saugiojo tinklo galima pasiekti aukštesnius saugumo standartus. Iš tiesų, Aiškinamasis raštas suponuoja, kad „tinkle“ esančios darbo vietos bus saugios tik dėl to, kad „saugusis tinklas“ atskiriamas/sujungiamas su viešaisiais tinklais per "vartus", kurie esant reikalui "uždaromi" ar "atidaromi". Tokiu būdu Aiškinamasis raštas iš esmės teigia, Saugusis tinklas bus unikalus saugumo požiūriu tuo, kad Saugiojo tinklo tvarkytojas saugos Saugiojo tinklo interneto perimetrą (angl. *Internet peering*).

(15) Toks požiūris į tinklo saugumą per interneto „vartų“ apsaugą yra technologiškai pasenęs ir pakankamai ribotas. Norint užtikrinti tinklo saugumą turi būti kalbama apie saugumo užtikrinimą ir kituose „saugaus tinklo“ perimetruose, pvz. kompiuterinėse darbo vietose, naudojant bevieles technologijas ir t.t. Jeigu nebus užtikrinta kiekvienos prie Saugiojo tinklo prijungtos darbo vietos tinkama apsauga, užkrėsta kenksmingu programiniu kodu tokia kompiuterinė darbo vieta taps naujais "vartais" į visą Saugųjį tinklą, kurių niekas nesaugos. Ši pakenkta „saugiojo tinklo“ vieta bus pasiekiama iš interneto ir viešųjų tinklų (pvz. bevieliais ar mobiliaisiais tinklais). Būtent ši saugi tinklo prieigos kontrolė buvo (yra) vienas didžiausių VĮ „Infostruktūra“ valdomo SVDPT tinklo iššūkių, kuris niekada taip ir nebuvo galutinai išspręstas.

(16) Kadangi Saugaus tinklo saugumo lygmuo mažėja sulyg kiekviena prijungta darbo vieta (ypač su tokių darbo vietų prijungimu, kurios nevaldo jokios jautrios informacijos ir natūraliai nenusipelno adekvataus dėmesio), Saugaus tinklo saugumą įmanoma užtikrinti tik apribojant prieigą prie Saugiojo tinklo iki minimumo, t.y. tinklu turi galėti naudotis tik tie subjektai ir tik tos darbo vietos, kurios valdo jautrią informaciją ir/arba turi privilegijuotus prisijungimus prie informacinių sistemų ar valstybės registrų. Būtent tokį siūlymą riboti prijungiamų darbo vietų apimtį teikia Infobalt.

(17) ***Trečia***, toks prieigos prie tinklo „ribotumas“ (kuris užtikrina didesnį tinklo saugumą) sudaro esminį TESTA tinklo principą. Kaip galima matyti iš Europos Komisijos pateikiamos TESTA tinklo apžvalgos[5] (pvz. 4.2.2 skyrius), prie TESTA tinklo nėra jungiamos visos to pageidaujančios valstybės institucijos ir jų darbo vietos. Siekiant gauti prieigą prie TESTA tinklo būtina pirmiausiai paaiškinti paslaugų poreikį ir pagrįsti, kad tikrai toks prisijungimas jiems yra reikalingas (automatinė prieiga prie visų TESTA resursų nėra suteikiama, prieiga ribojama tik paraiškoje nurodytais resursais[6]):

> *„Administrations should start by clearly defining their needs for TESTA Services, basically why and what services are needed. TESTA is focusing on users that have high security and/or availability requirements. Information systems requiring less stringent service or security levels should consider other communication solutions such as the Internet.“*

(18) Šie Europos Komisijos paaiškinimai labai gerai parodo, kad Saugusis tinklas (jeigu jis kuriamas kaip tinklas užtikrinantis aukštesnį saugumo standartą) turi būti prieinamas tik ribotai darbo vietų kategorijai, kurios valdo jautrius valstybės duomenis. Šie Europos Komisijos paaiškinimai gerai iliustruoja ir pirmąjį Infobalt teiginį, kad to paties subjekto viduje įmanoma įrengti tinkamai apsaugotą perimetrą tarp darbo vietų naudojančių „saugųjį tinklą“ ir darbo vietų, naudojančių rinkoje teikiamas elektroninių ryšių paslaugas.

(19) ***Ketvirta***, tinklo „ribotos prieigos“ aspektas yra akcentuojamas ir įstatymo projekto rengėjų, tačiau nėra įtvirtintas siūlomose įstatymo projekto formuluotėse.

(20) Šiame kontekste reikia atkreipti dėmesį į Įstatymo projekto 43^2 str., kuriame teikiama nuoroda į tai, kad Saugiojo tinklo naudojimas bus privalomas tik „*valstybės ir savivaldybių institucijoms ir įstaigoms, kurios atlikdamos gyvybiškai svarbias valstybės funkcijas dalyvauja vykdant valstybines mobilizacines užduotis*“. Poreikis užtikrinti ribotą prieigą prie Saugiojo tinklo akcentuojamas ir Aiškinamajame rašte. Tokie teiginiai suponuoja idėją, kad Saugusis tinklas iš tiesų turėtų būti prieinamas tik ribotam subjektų skaičiui / ribotam darbo vietų skaičiui.

(21) Visgi analizuojant Įstatymo projekte numatytus ribojimus bei Aiškinamajame rašte išdėstytus teiginius, galima pastebėti, kad *de facto* prieiga prie Saugiojo tinklo bus užtikrinama labai plačiam subjektų / darbo vietų ratui, kurie nevaldo jokios bent kiek jautresnės informacijos:

---

[5] https://ec.europa.eu/isa2/sites/isa/files/testa_overview_-_july_2017.pdf

[6] https://ec.europa.eu/isa2/sites/isa/files/testa_overview_-_july_2017.pdf, 4.2.3 skyrius.

(i) Kaip liudija Aiškinamajame rašte nurodytų Vyriausybės nutarimų Nr. 256 ir 631 analizė, „*gyvybiškai svarbias valstybės funkcijas*“ vienokia ar kitokia apimtimi užtikrina labai daug valstybės ar savivaldybės finansuojamų subjektų, įskaitant pvz. visas kultūros įstaigas ar sveikatos priežiūros įstaigas. Net jeigu pripažintume, kad tokios įstatyme įvardintos įstaigos ir institucijos kaip kultūros įstaigos ar sveikatos priežiūros įstaigos iš tiesų valdo valstybei jautrios informacijos ir turi poreikį naudotis „Saugiuoju tinklu“ dėl poreikio užtikrinti tam tikras mobilizacines funkcijas, yra visiškai akivaizdu, kad mobilizacijos sėkmę užtikrinti informacija yra kaupiama tik keliose darbo vietose. Tuo tarpu absoliuti dauguma tokių institucijų / įstaigų darbo vietų neturi jokios informacijos, kurią reikėtų saugoti naudojant „Saugųjį tinklą“ – Krašto apsaugos ministerijos administruojamą saugumo sistemą.

(ii) Kad „*gyvybiškai svarbias valstybės funkcijas*“ užtikrinančių įstaigų ir institucijų sąvoka yra labai lanksti bei leidžia sukurti plataus masto valstybinį monopolį, kuris būtų analogas visiškai įprastoms rinkoje siūlomoms paslaugoms, leidžia manyti Aiškinamojo rašto 12 punkte pateikta informacija apie tinklo įrengimui reikiamas lėšas. Šiame punkte nurodoma, kad „Saugusis tinklas“ bus kuriamas SVDPT tinklo pagrindu prie kurio jau dabar yra prijungta 1300 (!) valstybės institucijų ir įstaigų. Šis teiginys suponuoja, kad visi esami SVDPT naudotojai neatlikus jokio papildomo vertinimo automatiškai taps „*gyvybiškai svarbių valstybės funkcijų*“ vykdytojais.

(iii) Apibrėžiant Saugiojo tinklo naudotojų sąrašą Įstatymo projekte kalbama apie tai, kad *pareigą* naudotis Saugiojo tinklo paslaugomis turės asmenys, turintys mobilizacines užduotis. Tačiau kartu nurodoma, kad Saugaus tinklo naudotojais gali tapti ir kitos valstybės ir savivaldybių įstaigos ir institucijos, jeigu yra „*būtinybė užtikrinti nacionalinį saugumą ar gynybą*“. Analizuojant šią išimtį nesunku suprasti, kad valstybės ar savivaldybės kontroliuojamų subjektų atžvilgiu „*būtinybės užtikrinti nacionalinį saugumą ar gynybą*“ samprata praktiškai neturi jokių ribų. Dėl to realybėje sprendimas dėl prijungimo prie Saugiojo tinklo priklausys išimtinai nuo „kompetentingos institucijos“ subjektyvaus sprendimo, kuris nebūtinai sieks įgyvendinti „ribotos“ prieigos principą.

(22) Šių argumentų kontekste Infobalt sutinka su Įstatymo projektų rengėjų principine idėja, kad prieiga prie Saugiojo tinklo turi būti ribota. Kita vertus, Infobalt siūlo numatyti tokio ribojimo principus įstatyme, t.y. įstatyme turi būti įtvirtintas principas, kad prieiga prie Saugiojo tinklo yra teikiama tik subjektams turintiems mobilizacines užduotis bei įtrauktiems į Saugiojo tinklo naudotojų sąrašą, savo ruožtu tokių subjektų lygmenyje prieiga prie Saugiojo tinklo teikiama tik tokioms darbo vietoms, kurios valdo saugomą informaciją ir/arba turi privilegijuotą prieigą prie saugomų informacinių išteklių ar valstybės registrų[7].

(23) ***Apibendrinant,*** Infobalt teikia tris pasiūlymus siejamus su Saugiojo tinklo naudotojų sąrašo ribojimu:

(i) Saugiojo tinklo naudotojų sąrašas turi būti tvirtinamas įstatymu (toks pasiūlymas grindžiamas principu, kad Konstitucinės teisės gali būti ribojamos tik įstatymo lygmens teisės aktais);

(ii) Saugiojo tinklo naudotojais gali būti tik asmenys, turintys mobilizacines užduotis ir įrašyti į Saugiojo tinklo naudotojų sąrašą, t.y. negali būti kitų įstaigų ir institucijų, kurios gali pasinaudoti Saugiuoju tinklu (toks pasiūlymas grindžiamas poreikiu užtikrinti Saugiojo tinklo saugumą, galimybe riboti Konstitucines teises tik įstatymu ir užtikrinant proporcingumo principo įgyvendinimą);

[7] T.y. turi teisę įrašyti, pakeisti arba panaikinti duomenis.

(iii) Prieiga prie Saugiojo tinklo turi būti teikiama ne institucijoms, bet institucijų kompiuteriniams resursams, kurie turi prieigą prie saugomos informacijos ir/arba privilegijuotą prieigą prie valstybės informacinių išteklių ar valstybės registrų. Šiuo tikslu įstatyme siūloma įtvirtinti „Saugomos informacijos“ bei „Privilegijuotos prieigos prie informacinių išteklių“ sąvokas (toks ribojimas grindžiamas poreikiu užtikrinti Saugiojo tinklo saugumą ir principu, kad Konstitucinės teisės gali būti ribojamos tik proporcingai siekiamam tikslui).

III. KRAŠTO APSAUGOS MINISTERIJOS, SAUGIOJO TINKLO TVARKYTOJO IR SAUGIOJO TINKLO NAUDOTOJŲ VAIDMUO UŽTIKRINANT SAUGIOJO TINKLO VEIKIMĄ BEI NAUDOJANTIS SAUGIOJO TINKLO PASLAUGOMIS

(24) Įstatymo projekto 43^2 str. numatoma, kad teikiant Saugiojo tinklo paslaugas dalyvaus dvi arba trys institucijos – Vyriausybė, Krašto apsaugos ministerija (Saugaus tinklo valdytojas) bei jos kontroliuojama biudžetinė įstaiga (Saugaus tinklo tvarkytojas).

(i) Vyriausybė arba jos įgaliota institucija (greičiausiai KAM) tvirtins Saugiuoju tinklu teikiamų paslaugų sąrašą ir paslaugų teikimo taisykles;

(ii) KAM tvirtins specialiuosius organizacinius ir techninius reikalavimus, taikomus saugiajam tinklui, ir Saugiojo tinklo nuostatus;

(iii) Visus šiuos teisės aktus įgyvendins ir paslaugas teiks Saugiojo tinklo tvarkytojas, kurio funkcijas vykdys į biudžetinę įstaigą pertvarkyta VĮ „Infostruktūra“.

(25) Infobalt įsitikinimu, šis „Saugaus tinklo“ organizavimo modelis turi trūkumų bent dviem aspektais.

(26) ***Pirma***, pagal šiuo metu siūlomą modelį Saugiojo tinklo paslaugų, kurių teikimas būtų monopolizuotas, sąrašą turėtų tvirtinti Vyriausybė ar jos įgaliota institucija (greičiausiai KAM). Šiuo atžvilgiu reikia atkreipti dėmesį, kad Konstitucijos 46 str. draudžia monopolizuoti rinkas, o bet koks konstitucinių teisių ribojimas gali būti vykdomas tik įstatymo lygmens teisės aktais. Analogišką reikalavimą nustato Konkurencijos įstatymo 4 str., kuris draudžia viešojo administravimo subjektams iškreipti konkurenciją savo priimamais sprendimais *inter alia* sprendimais monopolizuojančiais tam tikros paslaugos teikimą. Šios teisės nuostatos suponuoja, kad *visos* Saugiojo tinklo paslaugos turi būti konkrečiai išvardintos įstatyme, tuo tarpu Vyriausybės ar jos įgaliotos institucijos priimamuose teisės aktuose gali būti pateikiamas tik tokių paslaugų detalizavimas. Dėl šios priežasties Infobalt siūlo įtvirtinti baigtinį Saugiojo tinklo paslaugų sąrašą Įstatymo projekte, pavedant Vyriausybei ar jos įgaliotai kompetentingai institucijai tokį paslaugų sąrašą ir paslaugų teikimo taisykles detalizuoti.

(27) Šiame kontekste atkreipiame dėmesį, kad Priede Nr. 1 pateikiamose Įstatymo projekto korekcijose Infobalt perkėlė visas KAM pasiūlytas „standartines paslaugas“, kurios turėtų tapti baigtiniu Saugiojo tinklo paslaugų sąrašu, tačiau siūlo atsisakyti žodžio „kolektyvinė“ paslaugoje „kolektyvinė apsaugą kibernetinio saugumo priemonėmis“, kadangi „kolektyvinės“ apsaugos paslaugos turinys nėra aiškus – aiškios tik apsaugos priemonės. Kelios korekcijos buvo atliktos ir kitose paslaugų apibrėžimuose, tačiau išlaikant principinę KAM pasiūlytų „standartinių paslaugų“ apibrėžtį.

(28) ***Antra,*** Įstatymo projekte numatytas konkretus Saugiojo tinklo kūrimo modelis, kuriame KAM dalyvauja kaip standartus kurianti, o VĮ „Infostruktūra“ – kaip šiuos standartus įgyvendinanti institucija neužtikrina Saugiojo tinklo saugumo standartų keliais aspektais:

(i) *Nėra adekvačios kontrolės.* Siūlomas modelis pažeidžia „keturių akių principą“. Kaip standartus kurianti institucija, KAM neturi adekvačių pajėgumų atlikti tinkamą techninę VĮ „Infostruktūra“ teikiamų paslaugų kokybės kontrolę. Net jeigu tokius pajėgumus KAM susikurtų,

dėl egzistuojančio interesų konflikto KAM atliekama kontrolė būtų neadekvati siekiant užtikrinti aukšto lygio saugumo standartus (pvz. KAM nebūtų linkusi konstatuoti „Infostruktūros“ valdomo Saugiojo tinklo trūkumų, jeigu pati KAM neskyrė prašytų lėšų tokioms saugumo spragoms pašalinti; „Infostruktūra“ objektyviai nebus linkusi kritikuoti KAM parengtų organizacinių ir techninių standartų siekdama išvengti priešpriešos su savo steigėju; jeigu egzistuojančios saugumo spragos bus sukurtos KAM ir Infostruktūros bendro darbo rezultate ir tokių spragų šalinimui reikės pripažinti klaidą, tokios saugumo spragos bus maskuojamos, o ne sprendžiamos ir t.t.). Tokiame kontekste tampa akivaizdu, kad Įstatymo projektas siūlo sukurti tokį Saugiojo tinklo modelį, kuris savo esme pažeidžia vieną pagrindinių saugumo principų – „keturių akių principą“.

(ii) *Nėra modelio leidžiančio užtikrinti adaptuotą ir kompleksinį saugumą*. Įstatymo projektas suponuoja, kad visa atsakomybė už Saugiojo tinklo saugumo standartų įgyvendinimą tenka VĮ „Infostruktūra“. Toks modelis implikuoja bent kelias saugumo problemas.

KAM tvirtinamais saugumo standartais bus siekiama užtikrinti saugumą makro / tinklo lygmenyje nustatant visiems Saugiojo tinklo naudotojams vienodus saugumo standartus / modelius, kurie vėliau bus diegiami Saugiojo tinklo naudotojų lygmenyje. Visgi pasaulinėje praktikoje yra pripažįstama, kad aukščiausias saugumo lygis pasiekiamas, kai kiekviena organizacija naudoja specialiai jai sukurtus saugumo įrankius, atitinkančius jų specifines sistemas ir problemas. Šio principo logika yra pakankamai paprasta – paslaugų teikėjai, neadministruojantys informacijos subjekto galutinių informacinių sistemų, negali jų gerai išmanyti ir užtikrinti aukšto saugumo lygio, nes reikia išmanyti informacinių sistemų architektūrą, komponentų komunikaciją, vietas, kuriose yra svarbiausi duomenys "karūnos deimantai" ir daug kitų aspektų, kurie leidžia saugą organizuoti efektyviai. Tai reiškia, kad Įstatymo projekte siūlomas diegti standartinis Saugiojo tinklo modelis negalės įgyvendinti *adaptuoto saugomo* principo, kuris užtikrina adekvačią kibernetinę saugą.

Adaptuoto saugumo principas yra glaudžiai susijęs su *kompleksinio saugumo* principu. Kompleksinio saugumo principas reikalauja užtikrinti saugą visuose tinklo lygmenyse, įskaitant konkrečius serverius ir darbo vietas, kurios jungiamos prie tinklo. Aiškinamasis raštas iš esmės kalba tik apie saugos užtikrinimą „tinklo“ / „makro“ lygmenyje (kuriami „vartai“ per kuriuos tinklo valdytojai jungiasi prie viešųjų išteklių, o KAM ir Saugaus tinklo tvarkytojas organizuoja šių „vartų“ apsaugą nuo kibernetinių grėsmių). Visgi susikoncentruodamas į „tinklo“ apsaugą siūlomas modelis palieka be adekvataus dėmesio atskirus Saugaus tinklo naudotojus, kuriuose įdiegus piktavališkas programas gali būti sukuriami nauji, niekieno nesaugomi „vartai“ į Saugųjį tinklą. Kaip minėta, norint tinkamai įvertinti kiekvieno Saugaus tinklo naudojo informacines sistemas ir parinkti šioms sistemoms tinkamiausias saugos priemones būtina žinoti kiekvieno konkretaus Saugaus tinko naudotojo informacinių sistemų struktūrą. To padaryti kokybiškai centralizuotai diegiant visiems Saugaus tinklo naudotojams standartinius sprendimus nėra įmanoma – kad ir kokie būtų naujai kuriamos biudžetinės įstaigos resursai, sunku įsivaizduoti, kaip tokia biudžetinė įstaiga adaptuoja saugumo sprendimus kiekvienai iš 1300 institucijų / įstaigų, kurioms paslaugų teikimą planuoja perimti iš VĮ „Infostruktūros“[8]. Todėl siūlomas modelis pažeis kompleksinio saugumo principą ("Multi-Layer defence" arba "Defence in depth" saugos principas).

Trečiasis saugumo aspektas yra siejamas su Saugaus tinklo naudotojo ir Saugaus tinklo tvarkytojo tarpusavio sąveika. VĮ „Infostruktūra“ valdomas SVDPT nėra saugus *inter alia* dėl to, kad Saugaus tinklo naudotojui yra sukuriama tik įstatyminė pareiga nusipirkti SVDPT paslaugas. SVDPT naudotojai nežino nei kodėl šio pasaugos turi būti perkamos, nei kokius duomenis jie

[8] Šis skaičius įvardinamas Aiškinamajame rašte.

saugo. Savo ruožtu, neturėdami atsakomybės už duomenų saugumą (tik pareigą nusipirkti SVDPT paslaugas), SVDPT naudotojai sauga patys praktiškai nebesirūpina iki tol, kol kyla kibernetinis incidentas. Įstatymo projektas realiai siūlo įgyvendinti tokį patį modelį, kuris nekuria „savininkiškumo“ ir atsakomybės už savo valdomų duomenų apsaugą, bei natūraliai užprogramuoja saugumo spragas Saugaus tinklo naudotojų lygmenyje, kurių pašalinimo net pats efektyviausias Saugaus tinklo tvarkytojas negali užtikrinti. Sąmoningumą ir atsakomybę gali užtikrinti tik glaudus bendradarbiavimas (nuolatinis bendravimas, stebėjimas, auditavimas, operatyvus kylančių problemų sprendimas ir t.t.), tarp paslaugos teikėjo ir saugiojo tinklo naudotojo. Jokia biudžetinė įstaiga neturi tokių resursų, kurie galėtų užtikrinti tokią Saugiojo tinklo tvarkytojo ir Saugiojo tinklo naudotojo tarpusavio sąveiką, kurioje saugumu rūpintųsi abu subjektai.

(iii) *Nėra elemento, kuris užtikrintų saugos tobulėjimą*. Sprendžiant iš Aiškinamojo rašto, saugos tobulėjimas bus užtikrinamas Saugiojo tinklo valdytojui įsigijus pačią geriausią įrangą, galbūt papildoma įranga bus perkama Saugiojo tinklo tvarkytojo darbuotojams grįžus iš kvalifikacijos kėlimo kursų, dalį saugumo spragų Saugiojo tinklo tvarkytojas šalins gavęs informacijos iš užsienio partnerių.

Toks modelis *garantuoja* Lietuvos kibernetinio saugumo atsilikimą nuo bet kokių kibernetinių grėsmių tendencijų. Tam yra bent kelios priežastys.

Būdamas monopoliniu teikėju Saugiojo tinklo tvarkytojas įgys įrangą / technologijas iš tam skirtų asignavimų ir juos privalės naudoti iki šios infrastruktūros nusidėvėjimo laikotarpio pabaigos. Tik tuomet Saugiojo tinklo tvarkytojas galės gauti asignavimų naujos laikmečio tendencijas atitinkančios įrangos įsigijimui. Iš esmės tai reiškia, kad Lietuvos kibernetinė sauga bus siejama su Saugiojo tinklo tvarkytojo investicijų nusidėvėjimo laikotarpiais, o ne naujai kylančiais kibernetinės saugos iššūkiais. Net jeigu Saugiojo tinklo tvarkytojo darbuotojai turėtų naujų idėjų kaip padidinti kibernetinės saugos lygmenį, šios idėjos turės laukti įgyvendinimo iki naujų asignavimų skyrimo momento.

Šiame kontekste pakankamai keistai atrodo ir Aiškinamajame rašte pateikiama informacija apie tai, kad Lietuvos kibernetinės saugos lygis bus didinamas gaunant informacijos iš užsienio partnerių apie naujus kibernetinės saugos iššūkius. Užsienio partneriai iš tiesų gali paaiškinti Saugiojo tinklo tvarkytojui tam tikras tendencijas, tačiau (i) šios tendencijos yra bevertės, kai neturi lėšų diegti naujoms saugumo sistemoms; (ii) Saugiojo tinklo tvarkytojas gaus informacijos apie tendencijas iš vieno šaltinio, kai egzistuojant decentralizuotam modeliui tokią informacija būtų gaunama iš neriboto skaičiaus šaltinių; (iii) užsienio partneriai iš principo nieko nežino apie Lietuvoje įdiegtą Saugųjį tinklą ir, ypač, apie individualių vartotojų lygmeniu diegiamas saugumo sistemas, todėl jų pastabos geriausiu atveju bus labai apibendrintos ir nesiūlančios konkrečių sprendimų leidžiančių užtikrinti būtent Saugiojo tinklo saugumą.

Modernios tinklo saugumą užtikrinančius sistemos užtikrina savaiminį saugos tobulėjimą, kuris užtikrinamas per „keturių akių principą“ (auditai, standartų adaptavimas ir t.t.), galintį įgyti pačias įvairiausias formas. Pavyzdžiui, tobulėjimas gali būti užtikrinamas keliems Saugaus tinklo paslaugų teikėjams rotacijos būdu audituojant vienas kito darbą, kuriant „Bug Bounty“ programas, kuriose ribotas arba neribotas ratas asmenų gali ieškoti pažeidžiamų vietų saugumo sistemose ir apie juos kontroliuojamai informuoti informacinių sistemų savininkus.

Kaip minėta, įstatymo projektas nenumato nei „keturių akių“ principo, nei bet kokių kitų priemonių, leidžiančių didinti Saugiojo tinklo saugą.

(29) Atsižvelgdama į aukščiau nurodytus Įstatymo projektu siūlomo įtvirtinti Saugiojo tinklo modelio trūkumus, Infobalt siūlo įgyvendinti alternatyvų funkcijų pasiskirstymą tarp Seimo, Vyriausybės, KAM, Saugiojo tinklo tvarkytojo papildomai įtraukiant į modelio veikimą privačius paslaugų teikėjus. Siūlomas modelis yra grindžiamas žemiau nurodytų funkcijų pasiskirstymu:

(i) Seimas tvirtina baigtinį Saugiojo tinklo paslaugų sąrašą (toks pasiūlymas grindžiamas principu, kad Konstitucinės teisės gali būti ribojamos tik įstatymo lygmens teisės aktais);

(ii) Vyriausybė ar jos įgaliota institucija gali detalizuoti įstatyme numatytas Saugiojo tinklo paslaugas bei tvirtinti paslaugų teikimo taisyklės, tvirtinti organizacinius ir techninius reikalavimus Saugiajam tinklui ir reikalavimus, kurie turi būti užtikrinami Saugiojo tinklo susijungimo su kitais kompiuteriniais resursais perimetre;

(iii) Saugiojo tinklo paslaugų teikimas yra decentralizuojamas: paslaugas teikia konkurso būdu atrinkti paslaugų teikėjai, kuriems keliamus kvalifikacinius, patikimumo ar kitokius reikalavimus nustato Vyriausybė ar jos įgaliota institucija.

(iv) Saugiojo tinklo valdytojas („Infostruktūra“) yra kompetencijų centras. Jis:

- padeda Saugiojo tinklo naudotojams įsigyti teisės aktus atitinkančias paslaugas; pagalba gali būti konsultacinė (standartinių pirkimo dokumentų rengimas, konsultacijos viešojo pirkimo būdu, viešojo pirkimų procedūrų atlikimas pagal perkančiosios organizacinės išduotą įgaliojimą ir t.t.) arba konsoliduojanti kelių subjektų vykdomus pirkimus (veikti kaip centrinė perkančioji organizacija);

- turi prieigą prie visų Saugiojo tinklo paslaugų komponentų ar patalpų, tikrina kaip Saugiojo tinklo paslaugų teikėjai užtikrina saugumo reikalavimus, atlieka auditus, teikia privalomus nurodymus tiekėjams dėl Saugiojo tinklo paslaugų teikimo, naudojamų techninių ar organizacinių priemonių pakeitimų;

- atlieka bendrą Saugiojo tinklo stebėseną ir kiekvienais metais rengia ataskaitą Saugiojo tinklo valdytojui (KAM), kuriame išdėsto esamą Saugiojo tinklo saugomo situaciją ir teikia rekomendacijas dėl priemonių, kurias reikėtų papildomai diegti norint užtikrinti didesnį tinklo saugumą.

- pats teikia paslaugas toje apimtyje, kiek tokių paslaugų nėra įmanoma įsigyti rinkoje laikantis proporcingumo principo. Toks tiekimas užtikrina galimybę diegti ypatingai įslaptintas sistemas, kurios yra prieinamos tik valstybėms, jeigu tokių būtų.

(30) Infobalt įsitikinimu, toks decentralizuotas modelis leidžia pasiekti gerokai aukštesnį Saugiojo tinklo standartą nedarant jokios žalos KAM deklaruojamiems tikslams:

(i) Šis modelis užtikrina Saugiojo tinklo dinamišką prisitaikymą prie naujų iššūkių – KAM konstatavus poreikį išspręsti naujus kibernetinius iššūkius KAM pakaktų priimti papildomus standartus, o šių standartų įdiegimas per KAM nurodytus terminus taptų tiekėjų atsakomybe. Standartų diegimas vykdomas vienu metu visų institucijų atžvilgiu nesukuriant „butelio kaklelio“ efekto vienos biudžetinės įstaigos lygmenyje. Maža to, norint įdiegti naujus standartus nereikėtų laukti naujų asignavimų ir/arba esamos infrastruktūros nusidėvėjimo.

(ii) Šis modelis užtikrina tinkamą valstybės ir privačių subjektų bendradarbiavimą tose kompetencijų srityse, kurioje jie yra labiausiai pasirengę. Infostruktūra vykdytų valstybės institucijoms labiau įprastas funkcijas – koordinuoti, kontroliuoti ir stebėti, tuo tarpu privatūs

tiekėjai teiktų jiems įprastas funkcijas – užtikrinti paslaugų teikimą pagal savo kliento poreikius ir teisės aktų reikalavimus.

(iii) Šis modelis užtikrina „keturių akių“ principą. Privačių subjektų teikiamų paslaugų kokybę prižiūri Saugiojo tinko tvarkytojas, kuris turi prieigą prie visų sistemų ir turi teisę duoti privalomus nurodymus paslaugų teikėjams. Saugaus tinklo tvarkytojas kiekvienais metais atsiskaito Saugiojo tinklo valdytojui teikdamas objektyvią, interesų konflikto nesaistomą tinklo saugumo apžvalgą ir rekomendacijas dėl tinklo saugos tobulinimo. Savo ruožtu, Saugaus tinklo valdytojas (KAM) turi teisę reikalauti įgyvendinti vienas ar kitas priemones nesaistomas savo paties veiksmų diegiant Saugiojo tinklo elementus. Esant poreikiui, valstybės institucijos poįstatyminiais teisės aktais sukurti „šešių akių“ principą, kurio pagrindu papildomą auditą vienas kito atžvilgiu atliktų ir skirtingi Saugiojo tinklo paslaugų teikėjai (pvz. numatant „Bug Bounty“ sistemą).

(iv) Šis modelis užtikrinta adaptuoto saugumo ir kompleksinio saugumo principų įgyvendinimą. Saugiojo tinklo valdytojas ir tvarkytojas turi galimybe rūpintis tinklo saugumu „tinklo“ / „makro“ lygmeniu, patvirtinti pagrindinius saugumo standartus, kuriuos turi įdiegti Saugiojo tinklo naudotojai. Tuo tarpu privatūs Saugiojo tinklo paslaugų teikėjai gali skirti pakankamai dėmesio kiekvienam individualiam Saugiojo tinklo naudotojui adaptuodami šiuos sprendimus pagal konkrečiai šiam subjektui kylančius saugumo iššūkius. Ar diegiant adaptuoto saugomo standartus buvo užtikrinti teisės aktų nustatyti reikalavimai ir toliau kontroliuoti galėtų Saugiojo tinklo tvarkytojas.

(v) Šis modelis diversifikuoja riziką. Aiškinamajame rašte iš esmės nurodoma, kad kilus krizinei situacijai privatus paslaugų teikimas galėtų sutrikti dėl to, kad privatūs subjektai galėtų nuspręsti paslaugos tiesiog nebeteikti. Infobalt atkreipia dėmesį, kad paslaugas teikia žmonės, kurių motyvacija ir interesas tęsti paslaugų teikimą krizinių situacijų atveju yra subjektyvus ir analogiškas nepriklausomai nuo to, ar konkretus žmogus dirba privačiame ar valstybiniame sektoriuje. Kaip privatus verslas gali netekti paslaugų teikimą užtikrinančių žmonių, taip žmonių gali netekti ir valstybinis paslaugų teikėjas. Tokiame kontekste svarbiausia yra ne aiškintis, kurie žmonės bus lojalesni valstybei, bet diversifikuoti riziką ir užtikrinti galimybę perimti paslaugų teikimą sutrikus vienai iš Saugiojo tinklo veikimą užtikrinančių grandžių tiek tiekėjų, tiek geografiniame lygmenyje. Infobalt siūlomas modelis užtikrina mažiausiai kelių paslaugų teikėjų veikimą visoje šalyje, kurie turi supratimą apie Saugaus tinklo organizavimo principus ir galimybę pakeisti tuos paslaugų teikėjus, kurie krizinėje situacijoje užtikrinti paslaugų teikimo nebeturi galimybės. Tokio diversifikavimo KAM siūlomas modelis nesiūlo – sutrikdžius vieno tiekėjo funkcijas (pasišalinus kertiniams Saugiojo tinklo tvarkytojo žmonėms), saugumo sistema būtų sutrikdyta visoje šalyje vienu metu be galimybės užtikrinti pakeičiamumo.

(vi) Šis modelis sukuria tiesioginį sutartinį santykį tarp Saugaus tinklo naudotojo ir paslaugų teikėjo, kuris užtikrina didesnį paties Saugaus tinklo naudotojo atsakomybės už savo valdomos informacijos saugumą jausmą. Svarbu yra tai, kad šis santykis sukuriamas neprarandant sutaupymų, kuriuos valstybė tikisi sukurti pirkdama vieno pirkimo metu didesnius prekių / paslaugų kiekius. Šis santykis kuriamas neprarandant ir tinkamos paslaugų kokybės kontrolės, kadangi Saugaus tinklo tvarkytojas išlieka kaip priežiūros institucija turinčia neribotą prieigą prie visų Saugaus tinklo elementų ir galinčia duoti privalomus nurodymus Saugaus tinklo naudotojams ir paslaugų teikėjams.

(vii) Šis modelis nereikalauja įtraukti į paslaugų teikimą subjektų, kurie neatitinka kvalifikacinių ar kitokių parametrų – Vyriausybė ar jos įgaliota institucija turi teisę nustatyti tokius kvalifikacinius ar kitokius reikalavimus, kurie suteiktų pakankamo komforto dėl tiekėjų ir/arba konkrečių paslaugas teikiančių asmenų patikimumo. Kitaip tariant, valstybė gali nustatyti

tiekėjams ir jų darbuotojams tokius pačius standartus, kuriuos keltų Saugiojo tinklo tvarkytojo darbuotojams teikiantiems paslaugas tiesiogiai. Šiuo atžvilgiu negalima sutikti su Aiškinamajame rašte pateikiamu argumentu, kad privataus verslo dalyviai susidurs su sunkumais gaunant leidimą dirbti su slapta informacija (jeigu tokių reikėtų). Viena vertus, ne visa Saugiojo tinklo valdytojo ar tvarkytojo gaunama informacija turi būti perduodama Saugiojo tinklo paslaugų teikėjams siekiant pašalinti saugumo spragas; antra vertus, savo prigimtimi privatus verslas visuomet yra lankstesnis, todėl iškilus abejonių dėl vieno ar kito asmens patikimumo, jis pakeis tokį paslaugas teikiantį asmenį gerokai greičiau, nei tai padarytų valstybinis paslaugų teikėjas; trečia vertus, įstatymai jau dabar numato galimybę tiekėjams ir tiekėjų specialistams galimybę gauti leidimus susipažinti su įslaptinta informacija, todėl tokių leidimų gavimas nesudaro privačiam verslui bent kiek reikšmingos kliūties teikti Saugiojo tinklo paslaugas.

(viii) Šis modelis palieka erdvės situacijai, kuomet valstybė siekia diegti Saugiojo tinklo elementus, kurie nėra prieinami privatiems subjektams – tokius tinklo elementu tiekti, paslaugas teikti gali pats Saugiojo tinklo tvarkytojas.

(31) ***Apibendrinant,*** Infobalt teikia du esminius pasiūlymus, siejamus su Saugiojo tinklo organizaciniu modeliu:

(i) Visos Saugiajam tinklui priskiriamos paslaugos turi būti numatytos įstatymo lygmens teisės aktuose (toks pasiūlymas grindžiamas principu, kad Konstitucinės teisės gali būti ribojamos tik įstatymo lygmens teisės aktais);

(ii) Saugiojo tinklo paslaugų teikimas turi būti užtikrinamas kooperuojant valstybės ir privataus verslo išteklius: Saugiojo tinklo valdytojas (KAM) turi apibrėžti organizacinius ir techninius reikalavimus taikomus Saugiajam tinkui, šiuos reikalavimus turi užtikrinti teisės aktų reikalavimus atitinkantys privatūs subjektai atrinkti konkurso būdu, o Saugiojo tinklo tvarkytojas („Infostruktūra“) turi veikti kaip kompetencijų centras, koordinuojanti ir kontroliuojanti institucija.

IV. PASTABOS SUSIJUSIOS SU VALSTYBINIŲ DUOMENŲ CENTRŲ VEIKLĄ REGLAMENUOJANIČOMIS NUOSTATOMIS

(32) Įstatymo projektu taip pat siekiama sukurti valstybinių duomenų centrų monopoliją numatant, kad tokias paslaugas teiks valstybės kontroliuojamas subjektas. Savo poziciją dėl tokios monopolijos neteisėtumo Infobalt išdėstė 2018-06-18 dienos KAM adresuotame rašte, kuris pridedamas kaip Priedas Nr. 2. Infobalt prašo įvertinti 2018-06-18 dienos rašte išdėstytus argumentus svarstant dėl įstatymo projekto Nr. 18-9700.

(33) Kartu Infobalt atkreipia dėmesį į konkrečias Įstatymo projekto formuluotes, kurios mūsų nuomone yra suformuluotos nekorektiškai.

(34) ***Pirma***, Įstatymo projekte siūloma apibrėžti duomenų centro sąvoka suponuoja, kad valstybinis duomenų centras privalomai turi būti įrengtas „biudžetinės įstaigos patikėjimo teise valdomose patalpose“ ir turi būti valdomas būtinai „biudžetinės įstaigos“. Infobalt įsitikinimu, tokia sąvoka apibūdina iš anksto žinomo valstybinio duomenų centro valdytojo savybes, kurios neturi nieko bendro su valstybiniam duomenų centrui keliamais tikslais. Šiuo atveju akivaizdu, kad duomenų centras netampa saugesnis ar efektyvesnis dėl to, kad jis yra valdomas biudžetinės įstaigos teisinį statusą turinčio subjekto ar tai, kad jis yra įrengtas patikėjimo teise valdomose patalpose. Mūsų nuomone, šie kriterijai įvedami tik tuo tikslu, kad vieninteliu valstybei svarbaus duomenų centro valdytoju galėtų būti monopolinę teisę turinti valstybės įmonė. Savo nuomonę dėl tokios monopolijos teisėtumo Infobalt jau išdėstė 2018-06-18 dienos rašte.

(35) ***Antra,*** siekiant Įstatymo projekte suformuoti valstybinę monopoliją galimai liko neįvertinta aplinkybė, kad valstybės kibernetinio saugumo užtikrinimo tikslais viena valstybės jautrių duomenų kopiją turėtų būti laikoma ne Lietuvos Respublikos teritorijoje. Kitos valstybės teritorijoje bus neįmanoma užtikrinti valstybinio duomenų centro patalpų valdymo „patikėjimo teise“ ar apskritai eksploatuoti duomenų centrą kitos valstybės „biudžetinės įstaigos“ teisiniu statusu. Atitinkamai, jeigu bus nuspręsta išlaikyti valstybinio duomenų centro monopolį įtvirtinančias nuostatas (kam Infobalt nepritaria), siūlome apibrėžti „valstybinio duomenų centro“ sąvoką pabrėžiant tokio duomenų svarbą ir atliekamą vaidmenį, t.y. nurodant tokiam duomenų centrui keliamas užduotis, priskiriamas funkcijas, saugomą informaciją, bet ne valdytojo teisinę formą ir patalpų valdymo teisinius pagrindus. Mūsų nuomone, minimaliai „valstybino duomenų centro“ sąvokoje turėtų atsirasti nuoroda į tai, kad šis duomenų centras yra skirtas tik „valstybės informacinių išteklių centrinio registro (duomenų bazės) saugojimui“.

(36) ***Trečia***, kaip nurodoma Aiškinamajame rašte ir Įstatymo projekto 42^3 str. pagrindinė valstybinio duomenų centro užduotis yra siejama su mobilizacinių funkcijų įgyvendinimu. Kaip galima suprasti, krizinės situacijos atžvilgiu didesnis saugumas yra užtikrinamas tuomet, kai visi svarbiausi valstybės duomenys yra saugomi vienoje vietoje.

(37) Infobalt nėra karinė struktūra ir jai sunku įvertinti konkrečias karines strategijas. Tačiau intuityviai peršasi išvada, kad priešiškoms jėgoms yra gerokai lengviau susprogdinti, užpulti ar kitaip pakenkti centralizuotai, o ne decentralizuotai, saugomiems valstybės informaciniams ištekliams. Surinkus visų mobilizacines užduotis turinčių institucijų informacinius išteklius į vieną vietą, kurios lokacijos nuslėpti nuo priešiškų jėgų bus neįmanoma, pašalinti visos valstybės gebėjimą vykdyti mobilizacines užduotis taps gerokai lengviau. Viena karinė ataka vieno objekto atžvilgiu pačioje konflikto pradžioje užbaigtų bet kokius valstybės bandymus vykdyti mobilizaciją.

(38) Šiame kontekste Infobalt mano, kad mobilizacinių užduočių vykdymas Įstatymo projekte yra nurodomas tik kaip nelabai tinkamai parinktas pretekstas siekiant įtvirtinti valstybinę duomenų centrų paslaugų monopoliją pažeidžiant Konstitucijos 46 str. bei ES teisės nuostatas. Panašu, kad KAM siekė įrodyti, kad duomenų centro paslaugų monopolijos sukūrimas yra valstybės funkcija, todėl karinės grėsmės pretekstu siekia parodyti, kad valstybinė monopolija reikalinga kaip dalis pasirengimo kariniam konfliktui.

(39) ***Ketvirta***, valstybinio duomenų centro sąvoka yra susijusi su „duomenų centro“ sąvoka. Siūloma duomenų centrą apibrėžti, kaip „*patalpas, skirtas serverių ir (arba) registrų ir valstybės bei kitų informacinių sistemų įrangai laikyti.*“ Toks apibrėžimas yra pernelyg siauras. Jis siejamas tik su patalpomis, kuriose laikoma įranga. Visgi duomenų centras yra sudėtinga ir kompleksinė infrastruktūra, kuri apima maitinimo, gesinimo, vėdinimo, apsaugos sistemas, komutacines spintas, kabelių sistemas ir pan. Atitinkamai, jeigu bus nuspręsta išlaikyti valstybinio duomenų centro monopolį įtvirtinančias nuostatas (kam Infobalt nepritaria), visas šis infrastruktūrinis kompleksas turėtų atsispindėti „duomenų centro“ sąvokoje.

(40) Pastebėtina, kad Infobalt požiūris į valstybinių duomenų centrų kūrimą ir tokio sprendimo teisėtumą kardinaliai skiriasi nuo KAM teikiamų pasiūlymų. Infobalt yra įsitikinusi, kad tokios paslaugos turėtų būti perkamos iš rinkos dalyvių galinčių pasiūlyti paslaugas atitinkančias teisės aktuose nustatytus reikalavimus. Dėl šios priežasties, Infobalt siūlo atsisakyti tokios valstybinės monopolijos kūrimo.

V. PRAŠYMAS

(41) Apibendrinant, Infobalt prašo įvertinti Infobalt atsižvelgti į išdėstytas pastabas ir:

(i) iš esmės peržiūrėti Saugiojo tinklo organizavimo modelį pagal Infobalt pateiktus pasiūlymus, kuris leidžia pasiekti analogiškus tikslus efektyviau, skiriant mažesnius finansinius išteklius ir neribojant konkurencijos;

(ii) atsisakyti valstybinių duomenų centrų monopolijos įtvirtinimo

Priedai:

1. Infobalt pasiūlymai KAM pateiktam Įstatymo projektui.
2. 2018-06-18 Infobalt raštas adresuotas Krašto apsaugos ministerijai.

Asociacijos „Infobalt“ direktorius [pasirašyta el. parašu] Paulius Vertelka

Projekto
lyginamasis variantas

LIETUVOS RESPUBLIKOS VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ VALDYMO ĮSTATYMO NR. XI-1807 1, 2, 5 ir 6 STRAIPSNIŲ PAKEITIMO IR ĮSTATYMO PAPILDYMO 43^2 IR 43^3 STRAIPSNIAIS ĮSTATYMAS

2018 m. d. Nr.
Vilnius

1 straipsnis. 1 straipsnio pakeitimas

Pakeisti 1 straipsnio 3 dalį ir ją išdėstyti taip:

„3. Šis įstatymas taikomas valstybės institucijoms, valstybės įstaigoms, valstybės įmonėms, viešosioms įstaigoms, steigiančioms, kuriančioms ir (arba) tvarkančioms valstybės registrus (kadastrus) (toliau – valstybės registras), žinybinius registrus, valstybės informacines sistemas ir kitas informacines sistemas, finansuojamoms iš valstybės biudžeto, Valstybinio socialinio draudimo fondo biudžeto, Privalomojo sveikatos draudimo fondo biudžeto ir kitų valstybės pinigų fondų ir Lietuvos Respublikos viešojo administravimo įstatymo nustatyta tvarka įgaliotoms atlikti viešąjį administravimą. Šio įstatymo 8, 10, 11 (išskyrus šio įstatymo 11 straipsnio 2 dalies 2 ir 3 punktus) straipsniai, 12 straipsnio 1 dalis, 13, 14, 30–37, 39–44 straipsniai taikomi valstybės ir savivaldybių įmonėms, savivaldybių įstaigoms ir viešosioms įstaigoms, kuriančioms kitas informacinių technologijų priemones, kuriomis apdorojama informacija, valdoma valstybės ir savivaldybių įmonių, savivaldybių įstaigų ir viešųjų įstaigų, atliekančių teisės aktų joms nustatytas funkcijas, jeigu išlaidos, patirtos kuriant tokias informacinių technologijų priemones, yra finansuojamos iš valstybės biudžeto, Valstybinio socialinio draudimo fondo biudžeto, Privalomojo sveikatos draudimo fondo biudžeto ar kitų valstybės pinigų fondų arba jeigu apdorojant informaciją informacinių technologijų priemonėmis per valstybės informacinių sistemų ar registrų sąveiką ~~reikalinga~~ **reikia** gauti duomenis iš valstybės informacinių sistemų ir (arba) registrų. **Šio įstatymo 43^2, 43^3 straipsniai taikomi valstybės ir savivaldybių institucijoms ir įstaigoms.** Šioje dalyje nurodytos institucijos, įstaigos ir įmonės toliau šiame įstatyme bendrai vadinamos institucijomis.“

2 straipsnis. 2 straipsnio pakeitimas

1. Pakeisti 2 straipsnio 13 dalį ir ją išdėstyti taip:

„13. ~~Saugus~~ **Saugusis** valstybinis duomenų perdavimo tinklas **(toliau – Saugusis tinklas)** – ~~elektroninių ryšių tinklas, atskirtas ir apsaugotas nuo viešųjų elektroninių ryšių tinklų (interneto) bei neteikiamas viešai, skirtas visoms Lietuvos Respublikos valstybės ir savivaldybių institucijoms, įstaigoms ir įmonėms bei kitiems juridiniams asmenims, kuriuo jie gali saugiai teikti duomenis, bendradarbiauti su Europos Sąjungos institucijomis, užtikrinant duomenų mainų dalyvių tapatybės nustatymą, perduodamų duomenų konfidencialumą, vientisumą ir prieinamumą~~ **krašto apsaugos ministro įgaliotos biudžetinės įstaigos valdomas specialiuosius organizacinius ir techninius reikalavimus atitinkantis elektroninių ryšių tinklas, kuriuo gali naudotis tik šio įstatymo nustatyta tvarka įvardinti saugiojo tinklo naudotojai.**“

2. Papildyti 13 straipsnį 13^1 dalimi:

„13^1 . ~~Saugoma informacija – valstybės informaciniai ištekliai, kurie yra įtraukti į ypatingos svarbos ir svarbių valstybės informacinių išteklių registrą~~ Saugoma informacija – valstybės informaciniai ištekliai, kurie yra įtraukti į ypatingos svarbos ir svarbių valstybės informacinių išteklių registrą ir yra naudojami Valstybės ir savivaldybių institucijų ir įstaigų joms atliekant gyvybiškai svarbias valstybės funkcijas dalyvaujant valstybinių mobilizacinių užduočių vykdyme.“

3. Papildyti 13 straipsnį 13^2 dalimi:

„13[2]. Privilegijuota prieiga prie saugomų informacinių išteklių – Saugiuoju tinklu saugomų informacinių išteklių (informacinių sistemų ar valstybės registrų bei jų funkcijoms užtikrinti būtinų programinių ir techninių resursų) naudotojams suteiktos prieigos teisės, skirtos atlikti informacinių sistemų ar valstybės registrų funkcionavimo, palaikymo ir atstatymo veiksmus.“

3 straipsnis. 5 straipsnio pakeitimas

Pakeisti 5 straipsnio 4 dalies 3 punktą ir jį išdėstyti taip:

„3) valdo ~~Saugų valstybinį duomenų perdavimo~~ **Saugųjį** tinklą. ~~Krašto apsaugos ministras tvirtina Saugaus valstybinio duomenų perdavimo tinklo nuostatus ir, vadovaudamasis Vyriausybės patvirtintais kriterijais, atlyginimo už naudojimąsi Saugiu valstybiniu duomenų perdavimo tinklu dydį.~~

4 straipsnis. 6 straipsnio pakeitimas

Pripažinti netekusį galios 6 straipsnio 4 dalies 4 punktą.

~~4) tvarko Saugų valstybinį duomenų perdavimo tinklą ir teikia šio tinklo paslaugas;~~

5 straipsnis. Įstatymo papildymas 43[2] straipsniu

Papildyti įstatymą 43[2] straipsniu:

„**43[2] straipsnis. Saugusis tinklas**

1. Valstybės ir savivaldybių institucijos ir įstaigos, kurios atlikdamos gyvybiškai svarbias valstybės funkcijas dalyvauja vykdant valstybines mobilizacines užduotis ir yra įrašytos į Saugiojo tinklo naudotojų sąrašą (toliau – Saugiojo tinklo naudotojai), privalo naudotis tik Saugiuoju tinklu teikiamomis elektroninių ryšių paslaugomis ir jungtis prie viešųjų elektroninių ryšių tinklų tik per Saugųjį tinklą. Saugiojo tinklo naudotojų sąrašas tvirtinamas įstatymu.

2. Šio įstatyme 1 dalyje numatytas reikalavimas naudotis Saugiu tinklu taikomas tik tokia apimtimi, kiek tai yra būtina siekiant užtikrinti Saugomos informacijos apsaugą ir perdavimą tarp asmenų, turinčių prieigą prie Saugomos informacijos, bei užtikrinti tokių Saugiojo tinklo naudotojų (darbo vietų) kompiuterinių resursų veikimą, kurie turi Privilegijuotą prieigą prie saugomų informacinių išteklių.

3. Vyriausybė arba jos įgaliota institucija:

1) detalizuoja Saugaus tinklo paslaugų sąrašą, kuriam priskiriamas (i) nustatytos spartos duomenų perdavimas tarp Saugiojo tinklo naudotojų ir Saugomos informacijos; (ii) nustatytos spartos Saugomos informacijos prieiga prie viešųjų ryšių tinklų ir šios prieigos apsauga kibernetinio saugumo priemonėmis; (iii) Saugomos informacijos apsauga kibernetinio saugumo priemonėmis; (iv) sąveikos su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais užtikrinimas.

2) nustato specialiuosius organizacinius ir techninius reikalavimus taikomus Saugiajam tinklui;

3) nustato specialiuosius organizacinius ir techninius reikalavimus, kurie taikomi Saugaus tinklo sąveikai su kitais kompiuteriniais resursais;

4) nustato kvalifikacinius (techninius, organizacinius ir kitokius) reikalavimus Saugiojo tinklo paslaugas teikiantiems asmenims;

5) nustato Saugaus tinklo paslaugas teikiančių asmenų pareigas, kuriomis užtikrinamas bendradarbiavimas su Saugaus tinklo tvarkytoju bei kitais Saugaus tinklo paslaugų teikėjais užtikrinant kolektyvinę kibernetinę Saugaus tinklo naudotojų apsaugą;

6) nustato Saugaus tinklo tvarkytojo įgaliojimus, leidžiančius kontroliuoti kaip Saugaus tinklo paslaugas parduodantys asmenys laikosi nustatytų Saugaus tinklo techninių ir organizacinių reikalavimų.

4. Saugųjį tinklą tvarko krašto apsaugos ministro įgaliota biudžetinė įstaiga, kuri veikia kaip kompetencijų centras ir Saugiojo tinklo veikimą pagal teisės aktais nustatytus

reikalavimus užtikrinanti institucija. Įgyvendindamas šiuos įgaliojimus Saugiojo tinklo tvarkytojas:

1) konsultuoja Saugiojo tinklo naudotojus dėl techninių ir organizacinių reikalavimų, kurie turi būti užtikrinami perkant Saugiojo tinklo paslaugas;

2) teikia pagalbą perkančiosioms organizacijoms siekiančioms įsigyti Saugiojo tinklo paslaugas. Teikdamas tokią pagalbą Saugiojo tinklo tvarkytojas gali (i) konsultuoti ir kitais būdais padėti Saugiojo tinklo naudotojams įsigyti Saugiojo tinklo paslaugas, įskaitant dalyvavimą Saugiojo tinklo naudotojų viešųjų pirkimų komisijos darbe; (ii) tvirtinti standartinius pirkimo dokumentus, kuriais turėtų vadovautis Saugiojo tinklo naudotojai siekdami įsigyti Saugiojo tinklo paslaugas; (iii) padėti įgyti Saugiojo tinklo paslaugas, atlikdama pirkimų procedūras pagal Saugiojo tinklo naudotojo suteiktus įgaliojimus, (iv) konsoliduoti Saugiojo tinklo naudotojų vykdomus Saugiojo tinklo paslaugų pirkimus veikdama kaip centrinė perkančioji organizacija, pagal kelių perkančiųjų organizacijų išduotus įgaliojimus ar kitais teisiniais pagrindais.

3) kontroliuoja kaip teikiamos Saugiojo tinklo paslaugos. Įgyvendindamas šią teisę Saugiojo tinklo tvarkytojas turi teisę pareikalauti suteikti prieigą prie visų dokumentų, kurių pagrindu vykdomas Saugiojo tinklo įrengimas ar Saugiojo tinklo paslaugų teikimas, patekti į Saugiojo tinklo paslaugų teikimui naudojamas patalpas, specialiomis techninėmis ir programinėmis priemonėmis patikrinti ar Saugiojo tinklo paslaugų teikimas atitinka teisės aktuose nustatytus reikalavimus;

4) teikia privalomus nurodymus Saugiojo tinklo naudotojams ir Saugiojo tinklo paslaugų teikėjams dėl teisės aktuose nustatytų techninių ir organizacinių priemonių, kurias turi atitikti Saugiojo tinklo paslaugos, teisės aktuose nustatytų reikalavimų neatitinkančių prekių ar paslaugų pakeitimo ar pašalinimo;

5) atlieka bendrą Saugiojo tinklo stebėseną ir kiekvienais metais rengia Saugiojo tinklo valdytojui ataskaitą, kurioje įvertinamas Saugiajame tinkle perduodamos informacijos saugumas bei pateikiamos rekomendacijos dėl priemonių, kurias reikėtų įgyvendinti siekiant didinti Saugiojo tinklo saugumą ir Saugiojo tinklo paslaugų efektyvumą.

6) Saugiojo tinklo naudotojams tiekia tokias Saugiojo tinklo paslaugas, kurių neįmanoma įsigyti rinkoje dėl to, kad teikiant šias paslaugas yra naudojamos specialios technologijos prieinamos tik valstybės institucijoms. Saugiojo tinklo tvarkytojas teikia tokio pobūdžio paslaugas laikydamasis proporcingumo principo. Šis principas be kitą ko reiškia, kad tokias paslaugas Saugiojo tinklo tvarkytojas teikia tik tada, kai specialios technologijos yra objektyviai būtinos siekiant apsaugoti išskirtinai jautrius duomenis ar informaciją, ir teikiamos tik tokia apimtimi, kiek tai neišvengiamai reikalinga norint užtikrinti šių duomenų ir informacijos apsaugą ir nėra jokių kitų mažiau konkurenciją ribojančių priemonių leidžiančių pasiekti analogiškus tikslus.

4. Saugiojo tinklo naudotojams Saugiojo tinklo tvarkytojo teikiamos Saugiuoju tinklu teikiamų paslaugų sąraše nurodytos paslaugos teikiamos neatlygintinai. Išlaidos, patirtos dėl neatlygintinai Saugiuoju tinklu teikiamų paslaugų, finansuojamos iš Saugiojo tinklo tvarkymui skiriamų valstybės biudžeto lėšų ir (arba) kitų teisės aktuose nustatytų finansavimo šaltinių.

5. Valstybės ir savivaldybių institucijų ir įstaigų prisijungimo prie Saugiojo tinklo ir atsijungimo iš jo sąlygas, planą ir terminus tvirtina Vyriausybė ar jos įgaliota institucija.“

7 straipsnis. Įstatymo įsigaliojimas ir įgyvendinimas

1. Šis įstatymas, išskyrus šio įstatymo 4, 8 straipsnius ir šio straipsnio 2–5 dalis, įsigalioja 2019 m. sausio 1 d.

2. Lietuvos Respublikos Vyriausybė, jos įgaliota institucija ir krašto apsaugos ministras iki 2018 m. gruodžio 31 d. priima šio įstatymo 5 straipsnio įgyvendinamuosius teisės aktus.

3. Šio įstatymo 4 straipsnis įsigalioja 2019 m. liepos 1 d.

4. 2019 m. liepos 1 d. įsigalioja tokia šio įstatymo 43^2 straipsnio redakcija:

„43[2] straipsnis. Saugusis tinklas

1. Valstybės ir savivaldybių institucijos ir įstaigos, kurios atlikdamos gyvybiškai svarbias valstybės funkcijas dalyvauja vykdant valstybines mobilizacines užduotis ir yra įrašytos į Saugiojo tinklo naudotojų sąrašą (toliau – Saugiojo tinklo naudotojai), privalo naudotis tik Saugiuoju tinklu teikiamomis elektroninių ryšių paslaugomis ir jungtis prie viešųjų elektroninių ryšių tinklų tik per Saugųjį tinklą. Saugiojo tinklo naudotojų sąrašas tvirtinamas įstatymu.

2. Šio įstatyme 1 dalyje numatytas reikalavimas naudotis Saugiu tinklu taikomas tik tokia apimtimi, kiek tai yra būtina siekiant užtikrinti Saugomos informacijos apsaugą ir perdavimą tarp asmenų, turinčių prieigą prie Saugomos informacijos, bei užtikrinti tokių Saugiojo tinklo naudotojų (darbo vietų) kompiuterinių resursų veikimą, kurie turi Privilegijuotą prieigą prie saugomų informacinių išteklių.

3. Vyriausybė arba jos įgaliota institucija:

1) detalizuoja Saugaus tinklo paslaugų sąrašą, kuriam priskiriamas (i) nustatytos spartos duomenų perdavimas tarp Saugiojo tinklo naudotojų ir Saugomos informacijos; (ii) nustatytos spartos Saugomos informacijos prieiga prie viešųjų ryšių tinklų ir šios prieigos apsauga kibernetinio saugumo priemonėmis; (iii) Saugomos informacijos apsauga kibernetinio saugumo priemonėmis; (iv) sąveikos su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais užtikrinimas.

2) nustato specialiuosius organizacinius ir techninius reikalavimus taikomus Saugiajam tinklui;

3) nustato specialiuosius organizacinius ir techninius reikalavimus, kurie taikomi Saugaus tinklo sąveikai su kitais kompiuteriniais resursais;

4) nustato kvalifikacinius (techninius, organizacinius ir kitokius) reikalavimus Saugiojo tinklo paslaugas teikiantiems asmenims;

5) nustato Saugaus tinklo paslaugas teikiančių asmenų pareigas, kuriomis užtikrinamas bendradarbiavimas su Saugaus tinklo tvarkytoju bei kitais Saugaus tinklo paslaugų teikėjais užtikrinant kolektyvinę kibernetinę Saugaus tinklo naudotojų apsaugą;

6) nustato Saugaus tinklo tvarkytojo įgaliojimus, leidžiančius kontroliuoti kaip Saugaus tinklo paslaugas parduodantys asmenys laikosi nustatytų Saugaus tinklo techninių ir organizacinių reikalavimų.

4. Saugųjį tinklą tvarko krašto apsaugos ministro įgaliota biudžetinė įstaiga, kuri veikia kaip kompetencijų centras ir Saugiojo tinklo veikimą pagal teisės aktais nustatytus reikalavimus užtikrinanti institucija. Įgyvendindamas šiuos įgaliojimus Saugiojo tinklo tvarkytojas:

1) konsultuoja Saugiojo tinklo naudotojus dėl techninių ir organizacinių reikalavimų, kurie turi būti užtikrinami perkant Saugiojo tinklo paslaugas;

2) teikia pagalbą perkančiosioms organizacijoms siekiančioms įsigyti Saugiojo tinklo paslaugas. Teikdamas tokią pagalbą Saugiojo tinklo tvarkytojas gali (i) konsultuoti ir kitais būdais padėti Saugiojo tinklo naudotojams įsigyti Saugiojo tinklo paslaugas, įskaitant dalyvavimą Saugiojo tinklo naudotojų viešųjų pirkimų komisijos darbe; (ii) tvirtinti standartinius pirkimo dokumentus, kuriais turėtų vadovautis Saugiojo tinklo naudotojai siekdami įsigyti Saugiojo tinklo paslaugas; (iii) padėti įgyti Saugiojo tinklo paslaugas, atlikdama pirkimų procedūras pagal Saugiojo tinklo naudotojo suteiktus įgaliojimus, (iv) konsoliduoti Saugiojo tinklo naudotojų vykdomus Saugiojo tinklo paslaugų pirkimus veikdama kaip centrinė perkančioji organizacija, pagal kelių perkančiųjų organizacijų išduotus įgaliojimus ar kitais teisiniais pagrindais.

3) kontroliuoja kaip teikiamos Saugiojo tinklo paslaugos. Įgyvendindamas šią teisę Saugiojo tinklo tvarkytojas turi teisę pareikalauti suteikti prieigą prie visų dokumentų, kurių pagrindu vykdomas Saugiojo tinklo įrengimas ar Saugiojo tinklo paslaugų teikimas, patekti į Saugiojo tinklo paslaugų teikimui naudojamas patalpas, specialiomis techninėmis ir

programinėmis priemonėmis patikrinti ar Saugiojo tinklo paslaugų teikimas atitinka teisės aktuose nustatytus reikalavimus;

4) teikia privalomus nurodymus Saugiojo tinklo naudotojams ir Saugiojo tinklo paslaugų teikėjams dėl teisės aktuose nustatytų techninių ir organizacinių priemonių, kurias turi atitikti Saugiojo tinklo paslaugos, teisės aktuose nustatytų reikalavimų neatitinkančių prekių ar paslaugų pakeitimo ar pašalinimo;

5) atlieka bendrą Saugiojo tinklo stebėseną ir kiekvienais metais rengia Saugiojo tinklo valdytojui ataskaitą, kurioje įvertinamas Saugiajame tinkle perduodamos informacijos saugumas bei pateikiamos rekomendacijos dėl priemonių, kurias reikėtų įgyvendinti siekiant didinti Saugiojo tinklo saugumą ir Saugiojo tinklo paslaugų efektyvumą.

6) Saugiojo tinklo naudotojams tiekia tokias Saugiojo tinklo paslaugas, kurių neįmanoma įsigyti rinkoje dėl to, kad teikiant šias paslaugas yra naudojamos specialios technologijos prieinamos tik valstybės institucijoms. Saugiojo tinklo tvarkytojas teikia tokio pobūdžio paslaugas laikydamasis proporcingumo principo. Šis principas be kitą ko reiškia, kad tokias paslaugas Saugiojo tinklo tvarkytojas teikia tik tada, kai specialios technologijos yra objektyviai būtinos siekiant apsaugoti išskirtinai jautrius duomenis ar informaciją, ir teikiamos tik tokia apimtimi, kiek tai neišvengiamai reikalinga norint užtikrinti šių duomenų ir informacijos apsaugą ir nėra jokių kitų mažiau konkurenciją ribojančių priemonių leidžiančių pasiekti analogiškus tikslus.

4. Saugiojo tinklo naudotojams Saugiojo tinklo tvarkytojo teikiamos Saugiuoju tinklu teikiamų paslaugų sąraše nurodytos paslaugos teikiamos neatlygintinai. Išlaidos, patirtos dėl neatlygintinai Saugiuoju tinklu teikiamų paslaugų, finansuojamos iš Saugiojo tinklo tvarkymui skiriamų valstybės biudžeto lėšų ir (arba) kitų teisės aktuose nustatytų finansavimo šaltinių.

5. Valstybės ir savivaldybių institucijų ir įstaigų prisijungimo prie Saugiojo tinklo ir atsijungimo iš jo sąlygas, planą ir terminus tvirtina Vyriausybė ar jos įgaliota institucija.“

5. Krašto apsaugos ministras iki 2019 m. birželio 30 d. priima šio įstatymo 4 straipsnio ir šio straipsnio 4 dalimi keičiamo įstatymo 43^2 straipsnio 2 dalies įgyvendinamuosius teisės aktus.

8 straipsnis. Įstatymo taikymas

1. Saugiojo tinklo naudotojai prijungiami prie Saugiojo tinklo ne vėliau kaip per trejus metus nuo įtraukimo į Saugiojo tinklo naudotojų sąrašą dienos.

2. Saugiojo tinklo naudotojai, iki šio įstatymo įsigaliojimo sudarę elektroninių ryšių paslaugų teikimo sutartis, turi teisę nesinaudoti Saugiojo tinklo paslaugomis iki sutarties termino pabaigos.

Skelbiu šį Lietuvos Respublikos Seimo priimtą įstatymą.

Respublikos Prezidentas

Lietuvos Respublikos krašto apsaugos ministerijai 2018-06-18 Nr.20180618/01

Kopija:

Lietuvos Respublikos Vyriausybės kanceliarijai
Lietuvos Respublikos ūkio ministerijai
Lietuvos Respublikos susisiekimo ministerijai
Lietuvos Respublikos finansų ministerijai
Lietuvos Respublikos teisingumo ministerijai
Lietuvos Respublikos vidaus reikalų ministerijai
Lietuvos Respublikos konkurencijos tarybai
Europos teisės departamentui prie Lietuvos Respublikos teisingumo ministerijos

Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 4, 5, 6, 22 ir 39 straipsnių pakeitimo ir įstatymo papildymo 43(2) ir 43(3) straipsniais įstatymo projekto

Nacionalinio informacinių ir ryšių technologijų (toliau – IRT) sektoriaus asociacija „Infobalt“ (toliau - Infobalt) teikia pastabas ir nuomonę dėl 2018 m. birželio 13 d. Lietuvos Respublikos krašto apsaugos ministerijos Lietuvos Respublikos Vyriausybei pateikto Nutarimo projekto „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 4, 5, 6, 22 ir 39 straipsnių pakeitimo ir įstatymo papildymo 432 ir 433 straipsniais įstatymo, Lietuvos Respublikos informacinės visuomenės paslaugų įstatymo Nr. X-614 4, 15, 16, 17, 18, 20, 21 ir 22 straipsnių pakeitimo įstatymo, Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatymo Nr. VIII-1524 7, 18 ir 20 straipsnių pakeitimo įstatymo, Lietuvos Respublikos administracinių nusižengimų kodekso 589 straipsnio pakeitimo įstatymo projektų pateikimo Lietuvos Respublikos Seimui“ Nr. Nr. 18-7357. Šiame nutarime siūloma pritarti Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 4, 5, 6, 22 ir 39 straipsnių pakeitimo ir įstatymo papildymo 43^2 ir 43^3 straipsniais įstatymo projektui (toliau - Projektas) ir jį pateikti Lietuvos Respublikos Seimui.

Pastaba Nr. 1. dėl Projekto derinimo su suinteresuotomis šalimis.

Lietuvos Respublikos teisėkūros pagrindų įstatymo 3 straipsnis nustato imperatyvius reikalavimus, keliamus teisėkūroje dalyvaujantiems subjektams, siekiant sukurti vientisą, nuoseklią, darnią ir veiksmingą teisės sistemą. Šio įstatymo 3 straipsnio 2 punkto 4 dalis nurodo, kad teisėkūroje vadovaujamasi *atvirumo ir skaidrumo* principu, kuris reiškia „*kad teisėkūra turi būti vieša, su bendraisiais interesais susiję teisėkūros sprendimai negali būti priimami visuomenei nežinant ir neturint galimybių dalyvauti, valstybės politikos tikslai, teisinio reguliavimo poreikis ir teisėkūroje dalyvaujantys subjektai turi būti žinomi, visuomenei ir interesų grupėms sudarytos sąlygos teikti pasiūlymus dėl teisinio reguliavimo visose teisėkūros stadijose, taip pat turi būti žinomi teisės aktų projektų rengimą inicijavę, teisės aktų projektus parengę, numatomo teisinio reguliavimo poveikio vertinimą atlikę subjektai ir teisinio reguliavimo stebėseną atliekantys subjektai*“.

Asociacija INFOBALT
Mokslininkų g. 2A-128, 08412 Vilnius
Interneto svetainė http://www.infobalt.lt
Tel. (8-5) 262 26 23
El. paštas office@infobalt.lt
A.s. LT74 7400 0112 3082 3814
AB „Danske Bank“ filialas,
Banko kodas 74000

Vadovaujantis Lietuvos Respublikos Vyriausybės darbo reglamento (toliau – Reglamentas) 25 punktu Vyriausybei teikiamiems teisės aktų projektams turi būti gautos išvados pagal kompetenciją iš ministerijų, Vyriausybės įstaigų, kitų valstybės ir savivaldybių institucijų ir įstaigų ar organizacijų.
Krašto apsaugos ministerijos pateiktas Projektas neatitinka Reglamento reikalavimų ir yra pateiktas jo nederinus bei negavus išvadų ar nuomonių iš Konkurencijos Tarybos, Lietuvos savivaldybių asociacijos, informacinių ir ryšių technologijų sektoriaus asociacijų.

Prašome pateikti Projektą Konkurencijos Tarybai, Europos teisės departamentui prie Lietuvos Respublikos teisingumo ministerijos, Lietuvos savivaldybių asociacijai ir kitoms institucijoms, įstaigoms ar organizacijoms, kurioms siūlomas naujas reguliavimas gali būti aktualus arba paskelbti projektus visuomenei susipažinti ir pastaboms pateikti.

Pastaba Nr. 2. dėl duomenų centrų ir duomenų perdavimo paslaugų monopolijos.
Infobalt teigia, kad pateiktu Projektu yra siūloma kurti valstybinę duomenų centrų ir duomenų perdavimo paslaugų monopoliją. Projekto iniciatoriai poreikį monopolizuoti *duomenų perdavimo* paslaugas ir *duomenų centrų* paslaugas grindžia tik tuo, kad pagal vieningus standartus centralizuotai teikiamos paslaugos yra saugesnės ir pigesnės už decentralizuotai perkamas paslaugas. Tačiau pateikto Projekto aiškinamajame rašte nėra atsakyta, kodėl tų pačių tikslų negalima pasiekti perkant paslaugas iš privačių rinkos dalyvių. Taip pat Projekto iniciatorių siūlymai nėra pagrįsti ekonominiais skaičiavimais bei saugumo analize. Projekto iniciatoriai nepateikia savo siūlymus pagrindžiančių įrodymų bei argumentų.

Detalių ir išsamų savo nuomonės pagrindimą Infobalt pateikia šio rašto Priede Nr.1. Infobalt yra įsitikinusi, kad (1) duomenų centrų ir duomenų perdavimo paslaugų teikimas yra „ūkinė veikla“, kuriai taikomos visos sąžiningą konkurenciją ginančios teisės normos; (2) paslaugų monopolizavimas pažeidžia Konstitucijos 46 str. reikalavimus; (3) paslaugų monopolizavimas pažeidžia Konkurencijos įstatymo 4 str. 2 d.; (4) monopolizavimo nepateisina tai, kad valstybė valdo subjektus teikiančius duomenų perdavimo ir duomenų centro paslaugas; (5) paslaugų monopolizavimas pažeidžia draudimą teikti valstybės pagalbą.

Prašome detaliai ir išsamiai atsakyti į šio rašto Priede Nr. 1 pateiktas pastabas ir argumentais pagrįsti Projekte teikiamus siūlymus.

Pastaba Nr. 3. dėl lėšų įgyvendinant Projekto siūlymus poreikio.
Lietuvos Respublikos teisėkūros pagrindų įstatymo 3 straipsnis nustato imperatyvius reikalavimus, keliamus teisėkūroje dalyvaujantiems subjektams, siekiant sukurti vientisą, nuoseklią, darnią ir veiksmingą teisės sistemą. Šio įstatymo Šio įstatymo 3 straipsnio 2 punkto 5 dalis, kad teisėkūroje vadovaujamasi *efektyvumo* principu, kuris reiškia „*kad rengiant teisės akto projektą turi būti įvertinamos visos galimos teisinio reguliavimo alternatyvos ir pasirenkama geriausia iš jų, teisės akte turi būti įtvirtinamos veiksmingiausiai ir ekonomiškiausiai teisinio reguliavimo tikslą leisiančios pasiekti priemonės, turi būti skelbiami ir įvertinami dėl teisinio reguliavimo gauti pasiūlymai, o teisėkūros veiksmai atliekami per protingus terminus*“.

Projekto iniciatorių parengto aiškinamojo rašto 12 punkte nurodoma, kad „*Projektuose siūlomoms nuostatoms įgyvendinti papildomų valstybės, savivaldybių biudžetų ir kitų valstybės įsteigtų fondų lėšų nereikės*“. Toks teiginys kelia pagrįstas abejones. Projektu siūloma suskurti reguliavimą, kurio pasėkoje

bus sukurtas naujas elektroninių ryšių tinklas, kuris (1) nuosavybės teise turės priklausyti valstybei; ir (2) bus nuo viešųjų elektroninių ryšių tinklų nepriklausomas.

Priėmus pateiktą Projektą valstybė turės skirti šį tinklą valdysiančiai biudžetinei įmonei asignavimus, kurie bus naudojami naujų elektroninių ryšių tinklų kūrimui bei jų administravimui. Ne mažiau svarbu, kad pagal pateiktą Projektą nėra aišku koks kiekis valstybės ir savivaldybių institucijų, įstaigų ar organizacijų privalės naudoti šį tinklą. Nesant kriterijų, kurias remiantis turėtų būti nustatomos institucijos, įstaigos ar organizacijos, kurioms privaloma naudoti šį elektroninių ryšių tinklą nėra aišku kiek investicijų pareikalaus tokio tinklo sukūrimas ir palaikymas.

Prašome Krašto apsaugos ministerijos pateikti kriterijus, kurias remiantis bus atrinktos institucijos, įstaigos ar organizacijos, kurios privaloma naudoti šį elektroninių ryšių tinklą arba pateikti sąrašą institucijų, įstaigų ar organizacijų, kurios Projekto iniciatorių vertinimu turės naudoti šį elektroninių ryšių tinklą.
Taip pat prašome Finansų ministerijos įvertinti ir pateikti nuomonę ar aiškinamajame rašte pateiktas valstybės, savivaldybių biudžetų ir kitų valstybės įsteigtų fondų lėšų poreikis įgyvendinti Projektu siūlomą reguliavimą yra pagrįstas, išsamus ir ekonomiškas.

Pastaba Nr. 4. dėl Projekto poveikio vertinimo.
Projekto iniciatoriai aiškinamajame rašte vertindami numatomo teisinio reguliavimo poveikį nurodo, kad priėmus Projektą, neigiamų pasekmių nenumatoma.

Šio rašto priede Nr.2 pateikiame išsamų siūlomo Projekto įtakos IRT sektoriui vertinimą. Infobalt požiūriu, valstybinių monopolijų sukūrimas konkurencingoje IRT rinkoje teikiamoms paslaugoms nėra ilgalaikė Lietuvos konkurencingumo didinimo strategija. Tai yra sąmoningas žingsnis didinti Lietuvos IRT sektoriaus atsilikimą. Valstybiniais monopoliais apribojus ir taip mažą Lietuvos IRT paslaugų rinką, valstybė apribos savo verslo galimybes vystyti valstybės sektoriui pritaikytas IT technologijas, kurios gali būti parduotos kitoms šalims, taip didinant aukštų technologijų prekių indelį bendrajame šalies produkte. Be to, pašalindama valstybės sektorių iš rinkos, Lietuva reikšmingai sumažins vidaus paklausą IRT produktams. Tai apribos IRT sektorius galimybes pasiekti pakankamą masto ekonomiją, kuri reikalinga siekiant kurti inovatyvius produktus privatiems rinkos dalyviams bei varžytis su globalios rinkos dalyviais.

Reikalaujame pateikti detalų ir išsamų numatomo teisinio reguliavimo poveikio vertinimą. Siūlomo reguliavimo poveikio vertinimas privalo apimti, bet neturi apsiriboti įtaka investicinei aplinkai, konkurencijai, ekonominei šalies situacijai ir IRT sektoriui, inovacijoms, darbo rinkai.

Pastaba Nr. 5 dėl užsienio šalių gerosios praktikos taikymo.
Krašto apsaugos ministerijos siūlomas *duomenų perdavimo* paslaugų ir *duomenų centrų* paslaugų teikimo modelis prieštarauja gerosioms saugumo etalonais laikomų organizacijų praktikomis. Kartu, nesivadovaujama kitų pažangių kaimyninių užsienio šalių pavyzdžiais.

NATO yra pasitvirtinusi debesijų kompiuterijos politiką, kuri numato, kad tik NATO konfidenciali informacija turi būti laikoma privačioje debesijos duomenų bazėje, kuri būtų valdoma pačios NATO arba aljanso valstybės narės. Tuo tarpu, visa kita informacija yra laikoma viešose arba hibridinėse debesijos duomenų bazėse. Kaimyninės Baltijos šalys taip pat yra numačiusios, kad tik ypatingos svarbos duomenys

būtų tvarkomi išimtinai nacionalinių vyriausybių. Kiti svarbūs valstybiniai duomenys yra laikomi duomenų centruose, kurie įrengti pasitelkiant privatų verslą, valstybei nustačius aiškius saugumo kriterijus. Išsamūs gerosios praktikos pavyzdžiai detaliai paaiškinami Priede Nr. 3

Prašome detaliai paaiškinti, kokių valstybių pavyzdžiais vadovaujasi Krašto apsaugos ministerija kurdama siūlomą valstybės informacinių išteklių konsolidavimo modelį, siekiant monopolizuoti dalį *duomenų perdavimo* ir *duomenų centrų* paslaugų rinkos.

Infobalt tikisi, kad bus tinkamai įvertinti siūlymai sukurti duomenų perdavimo ir duomenų centrų paslaugų monopolijas, tokių siūlymų atitikimas nacionaliniams ir ES teisės aktais ir bus susilaikyta nuo akivaizdžiai neteisėtų veiksmų atlikimo.
Infobalt ragina palaikyti ir Seimui pateikti Ūkio ministerijos įregistruotą Valstybės informacinių išteklių valdymo įstatymo pakeitimo projektą (projekto numeris 18-6725).
Infobalt yra įsitikinę, kad sprendimai dėl duomenų perdavimo ir duomenų centrų neturi būti skuboti. Siūlome bei prašome Krašto apsaugos ministerijos inicijuoti atvirą bei konstruktyvų dialogą dėl valstybės duomenų saugumo bei kibernetinės saugos.

Asociacijos INFOBALT direktorius [pasirašyta el. parašu] Paulius Vertelka

Priedas Nr.1

(1) Iniciatyvos kurti valstybinės duomenų centrų ir duomenų perdavimo paslaugų monopolijas kelia didelį Infobalt atstovaujamų bendrovių susirūpinimą. Todėl žemiau Infobalt pateikia argumentus pagrindžiančius, kad monopolijų kūrimas yra neteisėtas.

I. ESMINIAI KRAŠTO APSAUGOS MINISTERIJOS SIŪLOMŲ SUKURTI MONOPOLIJŲ POŽYMIAI

(2) Žemiau pateikiame esminius KAM siūlomos sukurti monopolijos požymius, kuriuos galima išskirti vertinant KAM pateiktus teisės aktų projektus bei jų aiškinamuosius raštus.

(3) Saugus tinklas (SVDPT): (i) priklauso valstybei nuosavybės teise; (ii) valdomas biudžetinės įstaigos; (iii) atitinka LRV nustatytus reikalavimus; (iv) sujungtas su TESTA tinklu; (v) nepriklausomas nuo viešųjų elektroninių ryšių tinklų; (vi) viešai neteikiamas; (vii) privalomai naudojamas LRV nurodytų institucijų.

(4) „Saugaus“ tinklo paslaugų monopolija kuriama LRV ir KAM priimamais poįstatyminiais teisės aktais. LRV sprendžia dėl to, kas pirks monopolines paslaugas ir nustato reikalavimus, kuriuos turi atitikti „saugus“ tinklas. Savo ruožtu, KAM paskiria monopolinės paslaugos teikėją, patvirtina nuostatus, „saugaus“ tinklo paslaugų sąrašą, paslaugų teikimo taisykles; institucijų prijungimo / atjungimo planus, užmokesčio už „saugaus“ tinklo paslaugų teikimą dydį. Užmokestis neturi viršyti paslaugų teikimo sąnaudų. Užmokestį už privalomas paslaugas mokės valstybės biudžetas, o už papildomas – paslaugų naudotojas.

(5) Valstybinis duomenų centras yra: (i) įrengtas biudžetinės įstaigos patalpose; (ii) eksploatuojamas biudžetinės įstaigos; (iii) įrašytas į valstybinių duomenų sąrašą.

(6) Duomenų centro monopolija taip pat kuriama LRV priimamais poįstatyminiais teisės aktais. LRV sprendžia dėl to, kas pirks monopolines paslaugas, paskiria monopolinės paslaugos teikėjus, tvirtina techninius reikalavimus duomenų centrams ir duomenų centrų paslaugų teikimo tvarką. Užmokestis už duomenų centrų teikiamas paslaugas mokamas iš valstybės biudžeto.

(7) KAM pateiktame aiškinamajame rašte monopolijų kūrimo poreikis grindžiamas šiomis aplinkybėmis:

(i) pigesnės paslaugos dėl centralizuojamo saugos užtikrinimo;

(ii) saugesnės paslaugos, nes (i) kolektyvinė gynyba yra efektyvesnė; (ii) teikiama standartizuota paslauga; (iii) užtikrinamas greitesnis reagavimas į kibernetinius incidentus; (iv) tinklas uždaras, gali naudotis tik ribotas asmenų ratas; (v) infrastruktūra valdoma koordinuotai; (vi) nacionalinis kibernetinio saugumo centras gali efektyviau taikyti kolektyvines gynybos priemones.

(8) **Įvertinus šiuos argumentus tampa aišku, kad KAM grindžia poreikį monopolizuoti *duomenų perdavimo* paslaugas ir *duomenų centrų* paslaugas tik tuo, kad pagal vieningus standartus centralizuotai teikiamos paslaugos yra saugesnės ir pigesnės už decentralizuotai perkamas paslaugas. Visgi teikdama siūlymą monopolizuoti paslaugų teikimą KAM taip ir neatsako, kodėl tų pačių tikslų negalima pasiekti perkant paslaugas iš privačių rinkos dalyvių.**

II. DUOMENŲ PERDAVIMO IR DUOMENŲ CENTRŲ PASLAUGŲ MONOPOLIŲ SUKŪRIMAS YRA NETEISĖTAS

(9) KAM siūlomas duomenų perdavimo ir duomenų centrų paslaugų monopolių sukūrimas prieštarauja nacionalinės ir ES teisės normoms. Išsamus KAM pasiūlymo teisinis vertinimas pateikiamas žemiau.

A. Duomenų centrų ir Duomenų perdavimo paslaugų teikimas yra „ūkinė veikla“, kuriai taikomos visos sąžiningą konkurenciją ginančios teisės normos

(10) Lietuvos Respublikos Konstitucijos, nacionalinės ir ES konkurencijos teisės taisyklių požiūriu „ūkinė veikla“ yra suprantama kaip veikla, kuria *norėtų* ir *galėtų* užsiimti privatūs subjektai[1]. Kaip nurodo Europos Komisija, „ūkinė veikla“ netampa valstybės funkcija vien dėl to, kad šia veikla užsiima valstybės institucijos[2] ar kad veikla vykdoma nesiekiant pelno[3]. Komisija taip pat nurodo, kad „ūkinės veiklos“ pobūdžio nepanaikina ir valstybės sprendimas monopolizuoti atitinkamos paslaugos teikimą[4] pavedant teikti tam tikras paslaugas savo kontroliuojamoms įmonėms. Šie Komisijos paaiškinimai yra aktualūs ir taikant nacionalines konkurenciją saugančias teisės normas, kadangi įstatymų leidėjas yra įtvirtinęs pareigą derinti Lietuvos Respublikos ir ES konkurencijos santykius reglamentuojančią teisę[5].

(11) Iš esmės tokia Komisijos pozicija reiškia, kad sprendžiant dėl KAM monopolizuoti siūlomų paslaugų priskyrimo „ūkinei veiklai“ turi būti klausiama, ar monopolizuojamas Duomenų centrų ir Duomenų perdavimo paslaugas *norėtų* ir *galėtų* teikti privatūs rinkos dalyviai[6].

(12) Duomenų centrų ir Duomenų perdavimo paslaugas Lietuvoje tiek privatiems, tiek viešiesiems subjektams jau teikia daugelis privačių rinkos dalyvių, kurie turi reikiamą programinę ir techninę įrangą, žmogiškuosius išteklius bei patirtį. Tokias paslaugas teikia Telia Lietuva, Bluebridge, Baltnetos Komunikacijos, Microsoft ir daugelis kitų ūkio subjektų. Infobalt nariai vieningai pareiškia, kad jie turi visas galimybes ir interesą teikti valstybės pasirinkto sudėtingumo Duomenų

[1] Komisijos pranešimas dėl Sutarties dėl Europos Sąjungos veikimo 107 straipsnio 1 dalyje vartojamos valstybės pagalbos sąvokos (2016/C 262/01), 14 p.
[2] Ten pat, 8 p.
[3] Ten pat, 9 p.
[4] Ten pat, 14 p.
[5] Konkurencijos įstatymo 1 str. 3 d.
[6] Toks ūkinės veiklos kriterijus taikomos ir Konkurencijos tarybos praktikoje. Žr. 2016-05-02 Konkurencijos tarybos nutarimą Nr. 2S-4/2016, “*Dėl Kauno miesto savivaldybės sprendimų, susijusių su Kauno miesto kapinių priežiūros ir laidojimo paslaugų teikimo organizavimu, atitikties Lietuvos Respublikos konkurencijos įstatymo 4 straipsnio reikalavimams*”.

centrų ir Duomenų perdavimo paslaugas užtikrinant tokį patį duomenų apsaugos standartą, kurio gali būti prašoma iš valstybinio monopolinės paslaugos teikėjo. To visiškai pakanka tam, kad šias paslaugas galima būtų laikyti „ūkine veikla“, kurios atžvilgiu taikomos visos sąžiningą konkurenciją saugančios taisyklės.

(13) Šiuo atžvilgiu papildomai pastebėtina, kad „ūkinės veiklos“ pobūdžio niekaip nekeičia aplinkybės, kurias KAM akcentuoja įstatymo projekte ir aiškinamajame rašte.

(i) **Tariamai „nemokamas“ paslaugų teikimas**. „Ūkinės veiklos“ egzistavimui neturi įtakos faktas, kad už Duomenų centrų ir Duomenų perdavimo paslaugas sumokės ne paslaugų gavėjas, o valstybės biudžetas. „Ūkinės veiklos“ pobūdis vertinamas pagal *savo esmę* nesisiejant su konkrečia užmokesčio už prekių/paslaugų teikimą forma ar šaltiniais. Todėl faktas, kad už paslaugų teikimą bus sumokama iš valstybės biudžeto neturi absoliučiai jokios įtakos „ūkinės veiklos“ pobūdžiui.

(ii) **Pelno nesiekimas.** „Ūkinės veiklos“ egzistavimui neturi įtakos faktas, kad monopolinės paslaugos bus teikiamos tik padengiant paslaugų teikimo kaštus (neviršijant sąnaudų)[7];

(iii) **„Saugaus tinklo“ sujungimas su TESTA tinklu.** Prijungimas prie TESTA tinklo KAM yra pristatomas kaip savybė, kurią gali užtikrinti tik valstybės kontroliuojamas subjektas. Tačiau taip nėra. Europos Komisijos paskelbtoje TESTA tinklo apžvalgoje[8] nurodoma, kad norint prisijungti prie TESTA tinklo yra keliami saugumo reikalavimai, kurie apibrėžiami techninėmis priemonėmis, politikomis, audito galimybe ir dvišalėmis sutartimis. Tačiau TESTA nuostatose nieko nesakoma apie tai, kad prisijungimą prie TESTA tinklo gali įrengti ir prižiūrėti tik valstybės kapitalo subjektas. Net jeigu toks ribojimas būtų (bet jo nėra) reikėtų atkreipti dėmesį, kad prie TESTA tinklo gali jungtis tik labai ribotas subjektų ratas, kuris turi pateikti atskirą prašymą Vidaus reikalų ministerijai (**VRM**) ir atitikti specialius reikalavimus nustatytus VRM įsakymu Nr. 1V-50[9]. Tai reiškia, kad pavienių subjektų poreikis prisijungti prie TESTA tinklo niekaip negali pateisinti visų valstybės institucijų naudojamų duomenų perdavimo paslaugų monopolizavimo.

Šiuo atžvilgiu pastebėtina, kad šis tariamas unikalus tinklo „saugumo“ elementas (prijungimas prie TESTA) jau buvo svarstomas Lietuvos vyriausiojo administracinio teismo spręstoje *Aukštadvario regioninio parko byloje*. 2017-09-11 sprendimu byloje Nr. I-12-502/2017 LVAT pripažino, kad valstybės monopolizuotos SVDPT paslaugos yra laikomos neteisėtai monopolizuota „ūkine veikla“. Toks sprendimas buvo padarytas

[7] Komisijos pranešimas dėl Sutarties dėl Europos Sąjungos veikimo 107 straipsnio 1 dalyje vartojamos valstybės pagalbos sąvokos (2016/C 262/01), 9 p.

[8] https://ec.europa.eu/isa2/sites/isa/files/testa_overview_-_july_2017.pdf

[9] Lietuvos Respublikos vidaus reikalų ministro 2004 m. vasario 24 d. įsakymas Nr. 1V-50 „Dėl Elektroninio keitimosi duomenimis su Europos Sąjungos ir valstybių narių administracijomis taisyklių patvirtinimo“ (Žin., 2004, Nr. 33-1078)

nepriklausomai nuo to, kad byloje nagrinėtos monopolinės paslaugos buvo priskirtos SVDPT – tinklui, kuris yra prijungtas prie TESTA tinklo.

(iv) **Kitos savybės nustatomos Duomenų perdavimo monopolinei paslaugai: nepriklausomas nuo viešųjų elektroninių ryšių tinklų, viešai neteikiamas, uždaras tinklas, atitinka LRV nustatytus reikalavimus**. Visos šios savybės nedaro Duomenų perdavimo paslaugos kažkuo unikalia, kurios *negalėtų* ir *nenorėtų* suteikti privatūs rinkos dalyviai. Tai yra visiškai įprasti techniniai parametrai, kuriuos valstybės nurodymu galėtų atitikti privatūs rinkos dalyviai. Jeigu reikėtų, privatūs rinkos dalyviai galėtų sukurti absoliučiai naują elektroninių ryšių tinklą su bet kokia įranga, paslaugų teikimo organizavimo principais ir kitais reikalavimais, kuriuos tik nurodytų valstybė.

Šiame kontekste būtina atkreipti dėmesį į viešoje erdvėje KAM išsakytus teiginius, kad privatūs subjektai negali užtikrinti saugumo dėl to, kad jie perka nesaugią įrangą, perka įrangą iš šalių, kurios užsiima šnipinėjimu ir t.t. Atkreipiame dėmesį, kad privatūs rinkos dalyviai gali nupirkti ar net pagaminti bet kokią valstybės pageidaujamą įrangą, pirkti įrangą arba nepirkti įrangos iš atskirų šalių – valstybė tik turi įvardinti, kokių konkrečiai parametrų paslaugos ji pageidautų.

(v) **Centralizuotas paslaugų teikimas, paslaugų teikimas pagal vienodą standartą.** Centralizuotas / standartizuotas paslaugų teikimo techninis reikalavimas, kurį vienodai gali įgyvendinti tiek KAM valdomas subjektas, tiek privatūs rinkos dalyviai. Privatūs subjektai gali suteikti paslaugas centralizuotai per vieną paslaugų teikėją, decentralizuotai per kelis paslaugų teikėjus veikiančius pagal vienodą standartą ar bet kaip kitaip. Be to, privatūs paslaugų teikėjai gali suteikti Nacionaliniam kibernetinio saugumo centrui tokias pačias galimybes prisijungti prie tinklo ir/ar jį kolektyviai saugoti, kaip kad tokią prieigą galėtų suteikti valstybinio monopolio valdytojas.

(vi) **Duomenų centro paslaugos?** Infobalt supratimu, KAM siūlyme monopolizuoti duomenų centro pasaugų teikimą nėra nurodoma absoliučiai jokio duomenų centro paslaugų unikalumo, todėl šias paslaugas galima laikyti ūkine veikla be jokios platesnės diskusijos.

(14) Apibendrinant, teikdama savo siūlymą sukurti valstybines monopolijas KAM nepateikė jokių argumentų patvirtinančių, kad monopolizuojamos „saugaus“ tinklo ar duomenų centro paslaugos nėra laikomos „ūkine veikla“. Tai reiškia, kad tokių paslaugų monopolizavimas turi atitikti sąžiningą konkurenciją saugančias Lietuvos ir Europos Sąjungos teisės aktų nuostatas. Mažiausiai, Konstitucijos 46 str., Konkurencijos įstatymo 4 str., Sutarties dėl Europos Sąjungos Veikimo 107 str. nuostatas

B. Paslaugų monopolizavimas pažeidžia Konstitucijos 46 str. reikalavimus

(15) Pripažinus, kad Duomenų perdavimo ir Duomenų centrų paslaugos pagal savo esmę yra laikomos „ūkine veika“, o KAM nedviprasmiškai tokias paslaugas siūlo monopolizuoti, tampa pakankamai

akivaizdu, kad toks siūlymas tiesiogiai pažeidžia Konstitucijos 46 str. numatytą draudimą monopolizuoti „ūkinę veiklą“: „*Įstatymas draudžia monopolizuoti gamybą ir rinką, saugo sąžiningos konkurencijos laisvę“*.

(16) Sąžiningos konkurencijos laisvė yra Konstitucijos ginama vertybė. Ji gali būti ribojama tik išimtiniais atvejais ir tik tada, jeigu tenkinamos trys esminės sąlygos: (i) konstitucinių laisvių apribojimas yra įtvirtintas įstatymo lygmens teisės aktuose; (ii) egzistuoja adekvati monopolizavimo priežastis, t.y. vienų konstitucinių laisvių ribojimas yra neišvengiamai reikalingas norint apsaugoti kitas konstitucines laisves; (ii) monopolizavimas yra proporcinga priemonė siekiamam tikslui, t.y. nėra mažiau ribojančių priemonių leidžiančių pasiekti analogiškus tikslus[10].

(17) LRV nutarimu kuriamas paslaugų monopolis netenkina nei vienos iš aukščiau paminėtų sąlygų.

(18) ***Pirma,*** paslaugų monopoliai (konstitucinių teisių apribojimas) yra įtvirtinami LRV ir KAM priimamuose poįstatyminio lygmens teisės aktuose, nors Konstitucijos 46 str. veikimas gali būti ribojamas tik įstatymo lygmens teisės aktais.

(19) Šiuo atžvilgiu pastebėtina, kad konstitucinių teisių ribų nustatymas negali būti deleguojamas kitoms institucijoms, kurios neturi teisės priimti įstatymo lygmens teisės aktų. Konkrečios monopolio ribos turėtų būti įtvirtintos *įstatyme* nepaliekant įstatymą įgyvendinančioms institucijoms galimybės keisti teisinio monopolio ribų savo priimamais *poįstatyminio* lygmens teisės aktais. Dėl šios priežasties, VIIVĮ įstatymo projekte nurodyti LRV ir KAM suteikti bendro pobūdžio įgaliojimai priimti monopolio ribas nustatančius poįstatyminius teisės aktus nesudaro tinkamo teisinio pagrindo, leidžiančio riboti Konstitucijos 46 str. garantuojamas teises. Kitaip tariant, KAM siūlo monopolius kurti poįstatyminiais teisės aktais, tuo ciniškai pažeidžiant Konstitucijos draudimą riboti konstitucines teises kitaip, nei įstatymo lygmens teisės aktais.

(20) ***Antra,*** monopolio kūrimas (Konstitucijos 46 str. ribojimas) galimas tik tada, kai kyla poreikis apsaugoti kitas Konstitucijos garantuojamas teises ir tik tokia apimtimi, kiek toks monopolizavimas yra būtinas.

(21) Panašu, kad Duomenų perdavimo ar Duomenų centrų paslaugos monopolizuojamos siekiant menamo „kaštų sutapymo“, kuris neva turėtų būti pasiektas valstybės institucijoms centralizuotai perkant šias paslaugas iš valstybinio monopolio valdytojo. Visgi menami „sutaupymai“ perkant paslaugas iš valstybės kontroliuojamo subjekto nėra Konstitucijos ginama vertybė. Todėl jie negali pateisinti Konstitucijos 46 str. garantuojamos sąžiningos konkurencijos laisvės ribojimo.

[10] Lietuvos Respublikos Konstitucinio Teismo 2006 m. gegužės 31 d. nutarimas "Dėl kvotinio cukraus eksporto", 2.2 punktas.

(22) ***Trečia,*** net jei manytume, kad Duomenų perdavimo ar Duomenų centrų monopoliu siekiama užtikrinti visuomenės saugumą, akivaizdu, kad monopolio kūrimas nėra proporcingas siekiamam tikslui.

(23) Konstitucinių teisių apribojimas galimas tik tada, jeigu nėra mažiau ribojančių priemonių leidžiančių pasiekti analogiškus tikslus (apsaugoti kitas Konstitucijos garantuojamas teises ir laisves)[11]. Vertinant atitikimą šiam reikalavimui turi būti keliami du klausimai: (i) ar Duomenų centrų ir Duomenų perdavimo paslaugų monopolizavimas yra neišvengiamai reikalingas norint užtikrinti visuomenės saugumą?; ir (ii) ar valstybė neišvengiamai turi patikėti tokių paslaugų teikimą valstybės kontroliuojamam subjektui?

(24) IT prekės ir paslaugos turi labai išskirtinius techninius parametrus. Jie pirkėjui leidžia apsispręsti, kokio saugumo jis norėtų, ir šį saugumą įvardinti techniniais parametrais. Pirkėjo formuluojami parametrai gali apimti reikalavimus IT įrangai, šios įrangos sujungimui, paslaugų teikimo organizavimui ir t.t.. Būtent taip (įvardindami pageidaujamus techninius parametrus) perka Duomenų perdavimo ir Duomenų centrų paslaugas privatūs subjektai, įskaitant subjektus, kurie valdo labai jautrius duomenis (pvz. bankai, prekybos tinklai, mokėjimo kortelių tinklai ir t.t). Tokia praktika leidžia manyti, kad visuomenės saugumas (jeigu dėl jo iš tiesų siekiama monopolizuojant paslaugas) gali būti pasiektas mažiau konkurenciją ribojančiomis priemonėmis: nustatant reikalavimus paslaugai, licencijuojant paslaugų teikėjus, kontroliuojant kaip šie laikosi nustatytų saugumo reikalavimų ir t.t. Todėl monopolijos kūrimas yra tiesiog neproporcinga priemonė ir netenkina vienos esminių konstitucinių teisių ribojimo sąlygų.

(25) Iš tiesų, nei KAM siūlomų teisės aktų projektuose, nei aiškinamajame rašte nėra nurodoma absoliučiai jokių reikalavimų, kurių negalėtų įgyvendinti privatus verslas. Savo ruožtu, įstatymo projekte suteikti įgaliojimai LRV patvirtinti techninius ir organizacinius Duomenų perdavimo ir Duomenų centrų paslaugų teikimo parametrus, kuriuos turės atitikti monopolinės paslaugos teikėjas tik patvirtina, kad valstybė geba apibrėžti reikalavimus monopolinėms paslaugoms, o privatūs subjektai galėtų šiuos reikalavimus tenkinti lygiai taip, kaip juos ketina tenkinti monopolinės paslaugos teikėjas.

(26) Net jeigu pripažintume, kad valstybės siekiamą saugumą gali užtikrinti tik vienas paslaugų teikėjas (su kuo Infobalt nesutinka), tokia išvada savaime dar nereiškia, kad šis paslaugų teikėjas būtinai turi būti valstybės kontroliuojamas subjektas. Infobalt įsitikinimu, paslaugų teikimo saugumas yra susijęs su paslaugos teikimo techniniais parametrais ir absoliučiai niekuo nesusijęs su tuo, ar paslaugų teikėjas yra kontroliuojamas valstybės ar privataus kapitalo. Paslaugų saugumo negarantuoja vien tas faktas, kad jas teikia valstybės kontroliuojamas subjektas, jeigu šis subjektas neskiria pakankamai lėšų įrangos modernizavimui, darbuotojų mokymams, dėmesio aukšto lygio profesionalų pritraukimui ir t.t.

C. Paslaugų monopolizavimas pažeidžia Konkurencijos įstatymo 4 str. 2 d.

[11] Lietuvos Respublikos Konstitucinio Teismo 2006 m. gegužės 31 d. nutarimas "Dėl kvotinio cukraus eksporto", 2.2 punktas.

(27) Konstitucijos 46 str. įtvirtintos sąžiningos konkurencijos laisvės apsaugą įgyvendina *inter alia* viešojo administravimo subjektams adresuotas Konkurencijos įstatymo 4 str. 2 d. numatytas draudimas iškreipti konkurencijos sąlygas rinkoje proteguojant vienus ūkio subjektus ir diskriminuojant kitus.

(28) Viešojo administravimo subjektų priimti teisės aktai vertinami kaip Konkurencijos įstatymo 4 str. 2 d. pažeidimas, kai nustatoma šių aplinkybių visuma: (i) viešojo administravimo subjekto teisės aktas ar kitoks sprendimas teikia privilegijas arba diskriminuoja atskirus ūkio subjektus ar jų grupes; (ii) dėl tokio sprendimo atsiranda ar gali atsirasti konkurencijos sąlygų skirtumų atitinkamoje rinkoje konkuruojantiems ūkio subjektams; (ii) skirtingos konkurencijos sąlygos nėra lemtos įstatymų reikalavimų vykdymo[12].

(29) Šiame kontekste svarbu pastebėti, kad Konkurencijos įstatymo 4 str. 2 d. požiūriu konkurencijos iškraipymus sukuriantys sprendimai gali būti pateisinami poreikiu vykdyti įstatymo reikalavimus tik tokia apimtimi, kuria viešojo administravimo subjektui nėra suteikiama galimybė pasirinkti elgesio modelio, t.y. priimdamas konkurenciją iškreipiantį sprendimą viešojo administravimo subjektas paprasčiausiai įvykdo iš įstatymo kylantį įpareigojimą[13]. KAM teikiamas įstatymo projektas nenumato jokio įpareigojimo LRV ar KAM dėl kuriamo monopolio turinio – kokios paslaugos monopolizuojamos, kas turi naudotis šiomis paslaugomis ir t.t. įstatymo projekte nėra nurodoma. Todėl bet kokie konkurencijos apribojimai, kuris kils monopolizuojant IRT paslaugas nekils iš įstatymų leidėjo valios – jie kils iš LRV ir KAM iniciatyvos ir pasirinkimų. Todėl šie pasirinkimai galės būti vertinami Konkurencijos įstatymo 4 str. 2 d. požiūriu nepriklausomai nuo to, kad priimti atitinkamus teisės aktus KAM ir LRV įpareigojo įstatymas.

(30) Kad sprendimu monopolizuoti Duomenų perdavimo ir Duomenų centrų paslaugas LRV ir KAM poįstatyminiais teisės aktais tenkins kitus Konkurencijos įstatymo 4 str. 2 d. reikalavimus, abejonių nekyla. KAM siūlo sukurti teisinį monopolį, kuris suprantamas kaip aukščiausias konkurencijos iškraipymo lygmuo. Pirmoji pažeidimo sąlyga yra tenkinama – KAM ir LRV yra viešojo administravimo subjektai. Antrojo ir trečioji sąlyga taip pat išpildoma – apibrėždami monopolinės teisės ribas LRV ir KAM privilegijuos monopolinės teisės turėtoją ir akivaizdžiai iškreips konkurencijos sąlygas IRT paslaugų rinkoje[14]. Todėl KAM pasiūlymas sukurti valstybines monopolijas pažeidžia ne tik Konstitucijos 46 str., bet ir Konkurencijos įstatymo 4 str. 2 d. reikalavimus.

D. Monopolizavimo nepateisina tai, kad valstybė valdo subjektus teikiančius Duomenų perdavimo ir Duomenų centro paslaugas

[12] LVAT administracinėse bylose Nr. A822-762/2009, Nr. A822-2563/2011, Administracinė jurisprudencija Nr. 21, 2011.
[13] Lietuvos vyriausiojo administracinio teismo 2017 m. birželio 13 d. nutartis administracinėje byloje Nr. A-2013-624/2017.
[14] Lietuvos vyriausiojo administracinio teismo 2015 m. birželio 15 d. nutartis administracinėje byloje Nr. A-1581-502/2015 Teismų praktika. 2015, 29, p. 195-247.

(31) KAM teikiamas projektas nenurodo, kas konkrečiai bus paskirti monopolinių paslaugų teikėjais. Tačiau įstatymas aiškiai nurodo, kad tai bus valstybės kontroliuojami subjektai.

(32) Infobalt įsitikinimu, siūlydama monopolizuoti komercines IRT paslaugas KAM vadovaujasi prielaida, kad valstybė turi galimybę teikti paslaugas *pati sau*, jeigu tik turi tokias paslaugas galinčią teikti įmonę. Visgi tokia prielaida (jeigu KAM ja vadovaujasi) nėra suderinama su Konstitucijos 46 str. ir Konkurencijos įstatymo 4 str. reikalavimais.

(33) Bylose susijusiose su savivaldybių sprendimais pavesti teikti tam tikrų paslaugų teikimą savo kontroliuojamiems subjektams teismai yra aiškiai nurodę, kad konkurencijos apribojimo (konkurso neskelbimo) nepateisina faktas, kad viešojo administravimo subjektas yra įsteigęs savo kontroliuojamą ūkio subjektą teikiantį jam reikiamas paslaugas[15]. Tokia teismų praktika leidžia daryti išvadą, kad Duomenų perdavimo ir Duomenų centrų paslaugų monopolizavimas negali būti vykdomas vien dėl to, kad valstybė *nori* teikti tokias paslaugas ir turi įsteigusi subjektą, kuris tokias paslaugas *galėtų* teikti.

E. Paslaugų monopolizavimas pažeidžia draudimą teikti valstybės pagalbą

(34) Draudimas iškreipti konkurencijos sąlygas yra formuluojamas ir ES teisės aktuose, kurie yra tiesiogiai taikomi Lietuvoje. Vienas jų – SESV 107(1) str. numatytas draudimas teikti valstybės pagalbą.

(35) Šis draudimas taikomas egzistuojant šių elementų teisinei sudėčiai: (i) valstybės priemonės teikia naudą „ūkio subjektui“; (ii) valstybės priemonė teikia *ekonominę naudą*, kurios ūkio subjektas nebūtų gavęs įprastomis rinkos sąlygomis; (iii) ekonominė nauda suteikiama panaudojant *valstybinius išteklius*, o naudos suteikimas priskirtinas *valstybės veiksmams*; (iv) priemonė yra *selektyvi*, t.y. pagalba suteikiama tik daliai ūkio subjektų; (v) priemonė gali *iškreipti konkurenciją* ir *paveikti prekybą tarp valstybių narių*.

(36) Vertinant KAM siūlomo įstatymo turinį abejonių nekyla dėl (i), (iii), (iv) ar (v) sąlygos. Komercinių paslaugų monopolizavimas teikia naudą „ūkio subjektui“, kadangi Duomenų paslaugų ir Duomenų perdavimo paslaugos savo esme yra „ūkinė veikla“. Už paslaugų teikimą monopolinės paslaugų teikėjui bus mokama iš valstybės biudžeto ar valstybinės kilmės subjektų biudžetų vadovaujantis valstybės institucijų – LRV ir KAM – nutarimais. Todėl biudžetinių lėšų nukreipimas monopolinės paslaugos teikėjui apima *valstybės išteklių* panaudojimą ir yra *priskirtinas valstybei*. Sprendimas yra selektyvus, kadangi nauda teikiama tik monopolinės paslaugos teikėjui. Konkurencijos ir prekybos tarp ES valstybių narių iškraipymai taip pat pasireikš, kadangi KAM siūlomu įstatymu yra kuriamas plataus masto monopolis, kuris išstumia

[15] Lietuvos Respublikos Konstitucinio Teismo 2015 m. kovo 5 d. nutarimas "Dėl konkurencijos atliekų tvarkymo paslaugų srityje": <...> *Šis reikalavimas gali būti nevykdomas tik objektyviai pateisinamu pagrindu; tokiu pagrindu nelaikytina vien tai, kad savivaldybė yra įsteigusi ūkio subjektą, veikiantį atliekų tvarkymo srityje*“. Lietuvos vyriausiojo administracinio teismo 2017 m. kovo 21 d. nutartis administracinėje byloje Nr. eA-215-552/2017.

iš rinkos tiek Lietuvos kapitalo, tiek kitų ES valstybių narių kapitalo subjektus (pvz. Telia Lietuva yra Švedijos kapitalo įmonė).

(37) Šiuo atžvilgiu Infobalt tik atskirai norėtų atkreipti dėmesį į (ii) teisinės sudėties elementą – ekonominės naudos suteikimą, kurios ūkio subjektas nebūtų gavęs įprastomis rinkos sąlygomis. Infobalt atkreipia dėmesį, kad monopolinės teisės suteikimas yra pripažįstamas ekonominės naudos suteikimu. Tokios teisės turėjimas suteikia aiškią ekonominę naudą, kadangi monopolio valdytojui teisės aktais rezervuojamos visos monopolio apimčiai priskiriamos pajamos nepatiriant jokių su tokios klientų bazės pritraukimu susijusių išlaidų. Savo ruožtu, monopolinės teisės suteikimas valstybės kontroliuojamam subjektui be konkurso reiškia, kad tokios naudos monopolio valdytojas nebūtų gavęs įprastomis rinkos sąlygomis. Tai, kad išimtinių teisių suteikimas gali būti laikomas ekonominio pranašumo suteikimu nurodoma ir Europos Komisijos paaiškinimų dėl valstybės pagalbos sąvokos 53-55 paragrafuose.

(38) Aukščiau nurodytų argumentų kontekste akivaizdu, kad KAM siūlomu įstatymo projektu ketinamas sukurti Duomenų perdavimo ir Duomenų centrų paslaugų monopolis pažeidžia SESV 107(1) str. numatytą draudimą teikti valstybės pagalbą.

F. Apibendrinimas dėl monopolio teisėtumo

(39) **Aukščiau pateikti argumentai leidžia daryti aiškią išvadą, kad KAM siūlomas sukurti Duomenų perdavimo ir Duomenų centrų paslaugų teisinis monopolis pažeidžia net tris savarankiškus teisinius pagrindus: Konstitucijos 46 str., Konkurencijos įstatymo 4 str. 2 d. ir SESV 107 str. 1 d. Savo ruožtu, KAM siūlomos sukurti monopolijos atitiktį aukščiau nurodytiems teisės aktams galės vertinti tiek nacionalinės, tiek ES institucijos.**

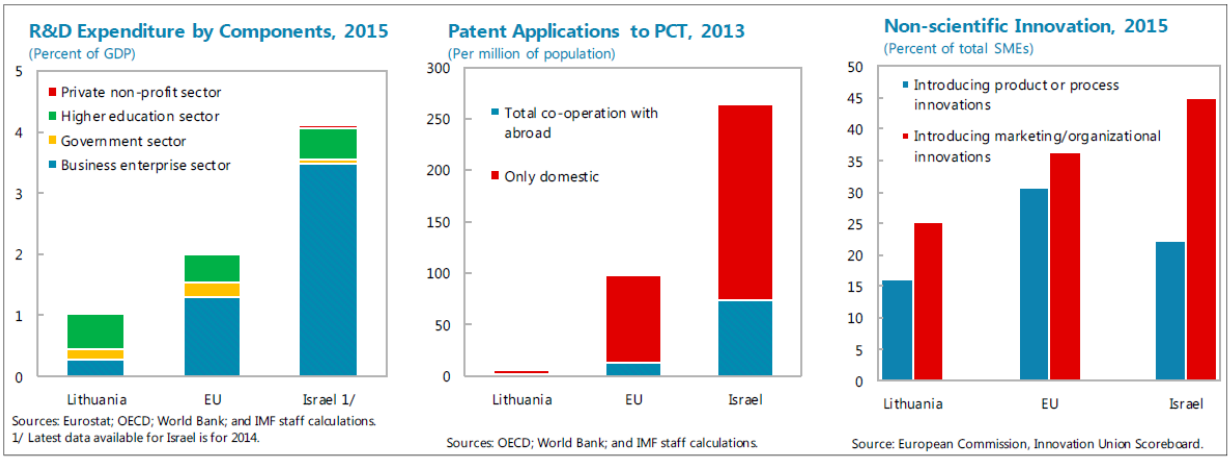
Priedas Nr.2

I. IRT PASLAUGŲ MONOPOLIJŲ KŪRIMAS PADIDINS LIETUVOS ATSILIKIMĄ IRT SEKTORIUJE

(1) Lietuva didžiuojasi vienu sparčiausių pasaulyje interneto ryšiu ar gerėjančiais IRT sektoriaus rezultatais. Visgi vertinant Lietuvos IRT sektoriaus pasiekimus ES ar pasaulinių tendencijų kontekste, tenka pripažinti, kad Lietuvos IRT sektoriaus konkurencingumas vis mažėja. Stojant IRT sektoriaus plėtrai, netenka prasmės ir Lietuvos didžiavimasis už valstybės lėšas įrengtu vienu greičiausiu pasaulyje internetu, – šios brangios infrastruktūros potencialas Lietuvoje lieka reikšmingai neišnaudotas dėl to, kad investicijos IRT sektoriuje vis dar lieka pakankamai ribotos.

(2) Infobalt požiūriu, valstybinių monopolijų sukūrimas konkurencingoje IRT rinkoje teikiamoms paslaugoms nėra ilgalaikė Lietuvos konkurencingumo didinimo strategija. Tai yra sąmoningas žingsnis didinti Lietuvos IRT sektoriaus atsilikimą. Valstybiniais monopoliais apribojus ir taip mažą Lietuvos IRT paslaugų rinką, valstybė apribos savo verslo galimybes vystyti valstybės sektoriui pritaikytas IT technologijas, kurios gali būti parduotos kitoms šalims, taip didinant aukštų technologijų prekių indelį bendrajame šalies produkte. Be to, pašalindama valstybės sektorių iš rinkos, Lietuva reikšmingai sumažins vidaus paklausą IRT produktams. Tai apribos IRT sektorius galimybes pasiekti pakankamą masto ekonomiją, kuri reikalinga siekiant kurti inovatyvius produktus privatiems rinkos dalyviams bei varžytis su globalios rinkos dalyviais.

(3) Šiame kontekste būtina pastebėti, kad žlugdydama privataus verslo galimybes kurti naujas technologijas Lietuva elgtųsi priešingai, nei Lietuvai rekomenduoja tarptautinės organizacijos, tokios kaip OECD ir Tarptautinis valiutos fondas. Šių organizacijų skelbiamais duomenimis, Lietuvoje neproporcingai didelę dalį išlaidų tyrimams ir išradimas skiria valstybės sektorius, kuriantis technologijas, kurios mažai reikalingos praktikoje. Kai tuo tarpu išsivysčiusiose valstybėse inovacijas vykdo privatus verslas[16].



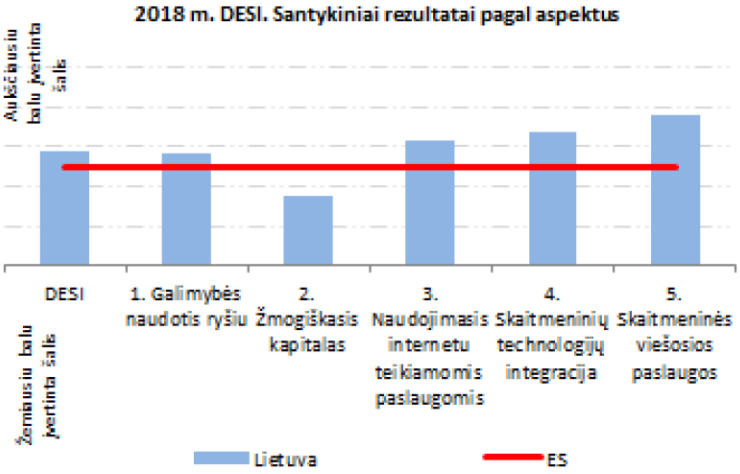
(4) Šiame kontekste nesunku numanyti, kad valstybinių monopolijų sukūrimas tokios statistikos nepagerins. Monopolijų valdytojas neturės absoliučiai jokių paskatų kurti naujų technologijų IRT sektoriuje. Dėl įstatyminės pareigos pirkti monopolines paslaugas, jos bus perkamos net, jeigu šios paslaugos bus atsilikusios nuo rinkos tendencijų šviesmečiais ir/arba absoliučiai netenkins viešojo sektoriaus poreikių.

[16] P. 14-15 of International Monetary Fund 2017 report on Lithuania (IMF Country Report No. 17/177). http://www.imf.org/en/Publications/CR/Issues/2017/06/30/Republic-of-Lithuania-2017-Article-IV-Consultation-Press-Release-and-Staff-Report-45018

Kurti ir eksportuoti naujų technologijų kitoms šalims valstybinio monopolio valdytojas neturės poreikio, nes jo funkcijos bus ribotos tik valstybinio sektoriaus poreikių tenkinimu. Savo ruožtu, valstybei vieną dieną suvokus, kad valstybinis monopolis nesuspėjo su dinamiškos IRT rinkos tendencijomis ir nubloškė Lietuvą į skaitmeninės ekonomikos paraštes, Lietuva turės nueiti labai ilgą kelią siekdama ištaisyti savo padarytą žalą. Lietuva pirks kitų šalių pagamintas IRT technologijas vien dėl to, kad veikiant valstybinėms monopolijoms Lietuvos IRT sektorius jau bus praradęs gebėjimus pasiūlyti valstybės sektoriui reikiamus produktus.

(5) Tokių dėsningumų kontekste, Infobalt yra nesuvokiama, kaip valstybinių monopolijų kūrimas koreliuoja su valstybės deklaruojamu tikslu didinti aukštų technologijų indelį Lietuvos ekonomikoje ir skatinti verslą investuoti į naujų technologijų kūrimą? Nesuvokiama ir tai, kaip kurdama valstybines monopolijas valstybė ketina sustabdyti emigraciją (ypač aukštą pridėtinę vertę kuriančių IRT specialistų emigraciją), kuri šiai dienai privedė Lietuvą prie demografinės krizės.

(6) Naujausi ES skelbiami Lietuvos skaitmeninės rinkos duomenys[17] teigia, kad Lietuvos skaitmeninės ekonomikos vystymąsi stabdo žmogiškojo kapitalo trūkumas.



(7) Šis rodiklis sako, kad Lietuvoje iš principo trūksta IRT specialistų, kurie galėtų kurti IRT technologijas. Taip yra todėl, kad IRT specialistų trūksta visame pasaulyje ir didelė dalis mūsų talentų keliauja dirbti į tas šalis, kurios gali pasiūlyti didesnį darbo užmokestį. Siekdama išlaikyti IRT specialistus Lietuvoje IRT sektoriaus bendrovės IRT specialistams moka dideles algas ir bando sudominti ambicingais projektais.

(8) Su visa pagarba viešojo sektoriaus dalyviams, reikėtų pripažinti, kad šiuo metu valstybės galimybės mokėti didesnius darbo užmokesčius ar kitaip motyvuoti savo darbuotojus yra labai ribotos.

(9) Tai galima iliustruoti pvz. skirtumu tarp rinkoje mokamo atlyginimo kibernetinės saugos specialistams ir atlyginimo, kuris mokamas VĮ „Infostruktūra“ darbuotojams.

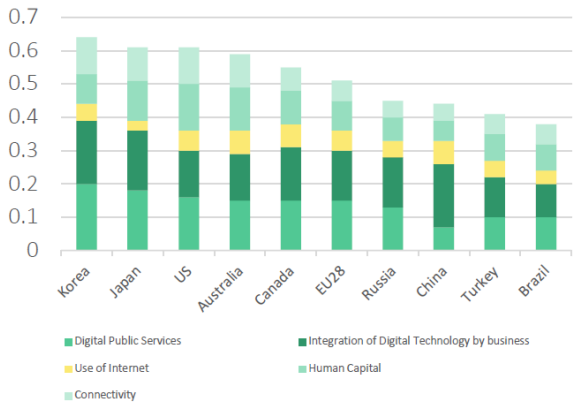
Kibernetinės saugos specialistai (atlyginimas, gross) turintys atitinkamą sertifikatą	VĮ „Infostruktūra“ darbuotojų atlyginimo duomenys[18] (2018 m. I ketvirtis)

[17] http://ec.europa.eu/information_society/newsroom/image/document/2018-20/lt-desi_2018-country-profile-lang_4AA80A21-0C1D-11AA-64D2CE84D72961F4_52356.pdf
[18] http://www.is.lt/lt/apie-mus/finasinnes-ataskaitos.html

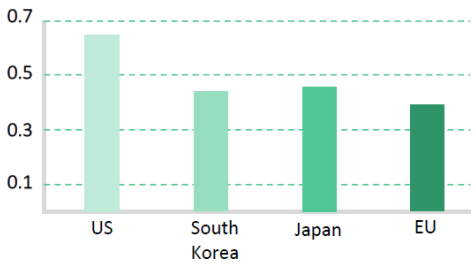
Vidutinės kvalifikacijos specialistai	2763–3947 eur/gross	Direktorius	2851 eur/gross
Aukščiausios kvalifikacijos specialistai	nuo 3947 eur/gross	Skyriaus vadovas	2132 eur/gross
		Vyresnysis inžinierius	2478 eur/gross
		Sistemų administratorius	1416 eur/gross
		Informacijos saugos ekspertas	1841 eur/gross

(10) Šie duomenys parodo, kad privačiame sektoriuje vidutinės kvalifikacijos kibernetinės specialistui mokamas atlyginimas *prasideda* nuo atlyginimo lygmens, kuris mokamas numanomo monopolinių paslaugų teikėjo vadovui. Šie duomenys labai aiškiai parodo, kad valstybė bent jau šiai dienai iš principo negali konkuruoti dėl tokios mobilios ir didelę paklausą pasaulyje turinčios darbo jėgos, kaip IRT specialistai. Todėl sukurdama valstybines monopolijas IRT paslaugoms valstybė sukurs dar didesnę žalą Lietuvos IRT rinkai. Tikimybė, kad valstybinio monopolio valdytojas sugebės pritraukti kvalifikuotus IRT specialistus valstybinės paslaugos teikimui yra labai maža. Savo ruožtu, neturėdamas galimybės IRT specialistams pasiūlyti dirbti su sudėtingais ir ambicingais viešojo sektoriaus projektais Lietuvoje, IRT specialistų išlaikyti neturės galimybės ir privatus verslas.

(11) Vertinant valstybinių monopolijų kūrimo siūlomą perspektyvą būtina atkreipti dėmesį į tai, kad Lietuvos IRT sektoriaus atsilikimas tampa vis aiškiau matomas statistiniuose rodikliuose. Lietuva dažniausiai savo išsivystymą vertina ES valstybių narių kontekste. Visgi toks vertinimas sukuria gerokai iškreiptą vaizdą, kai mes kalbame apie Lietuvos dalyvavimą globalioje IRT paslaugų rinkoje, kurioje ES rodikliai yra tik šiek tiek geresni, nei besivystančių šalių, tokių kaip Rusija, Turkija, Brazilija ar Kinija. Ši statistika rodo, kad norėdama būti globalia aukštų technologijų šalimi Lietuva neturi orientuotis į ES vidurkius, – Lietuva turi orientuoti į globalius rinkos standartus.



Šaltinis: International Digital Economy and Society Index (I-DESI) (CapGemini) data refer to 2015 or earlier



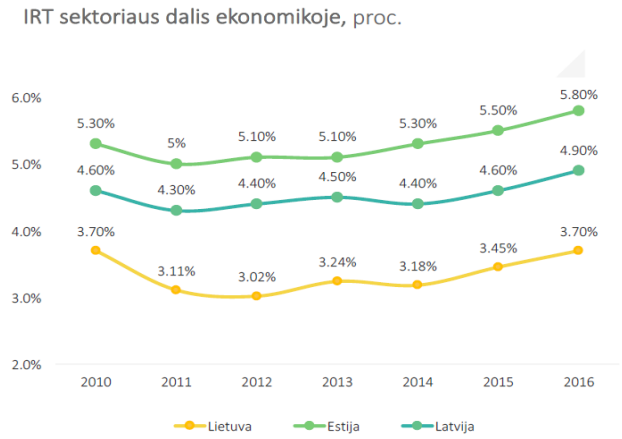
Intergration of digital technology by businesses : an international comparison

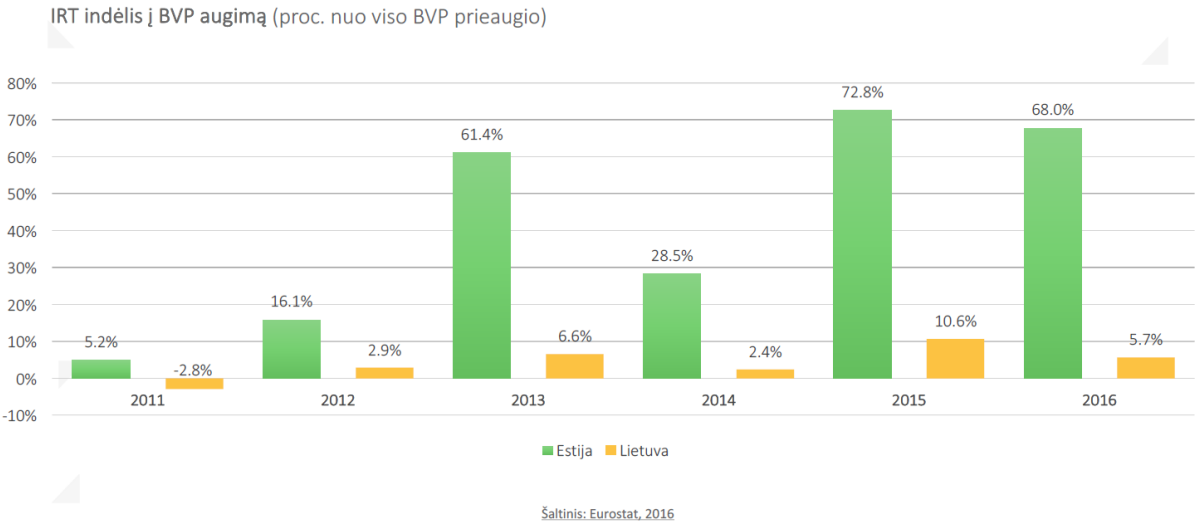
(12) Nepaisant to, netgi ES masto statistiniuose rodikliuose Lietuva yra tik stipri vidutiniokė turinti aiškią IRT sektoriaus konkurencingumo mažėjimo tendenciją. Tai iliustruoja ES sudaromas „Digital Economy and Society Index“, kuriame nuo 2014 metų Lietuvos IRT sektoriaus išsivystymo lygis nuosekliai mažėja. Jeigu

2014 m. Lietuva užėmė tarp ES valstybių narių 9 vietą, 2015 m. – 11, 2016 m. – 12, tai 2017 m. Lietuva jau užima 13 vietą tarp ES valstybių narių[19]. Kalbant apie Lietuvos pažangą kitų valstybių kontekste tarptautiniuose leidiniuose pabrėžiama, kad skaitmenizacijos lyderėmis yra laikomos Šiaurės šalys, tarp jų ir Estija. Tuo tarpu, kalbant apie Lietuvą paprastai yra sakoma tik tiek, kad Lietuva nuosekliai tolsta nuo šalių su išsivysčiusi IRT sektoriumi:

> *„Unless Lithuania, Latvia and Poland start to follow in the footsteps of Estonia, there is a risk of further polarization between BSR countries. The Nordic countries are still ahead of the other countries in the region, but Estonia's development is strong and if it continues at its current pace, it will soon catch-up with, or even surpass, the Nordics. If Poland, Latvia and Lithuania do not pick up pace, this means that there will be further polarization between the countries in the BSR.“*[20]

(13) Iš tiesų, jau šiai dienai Lietuva labai reikšmingai atsilieka netgi nuo mūsų artimiausių kaimynių. Tai akivaizdžiai matosi IRT sektoriaus indelio į valstybės ekonomiką statistiniuose duomenyse, kuriuos pateikia Lietuvos, Latvijos ir Estijos oficialios statistikos institucijos:

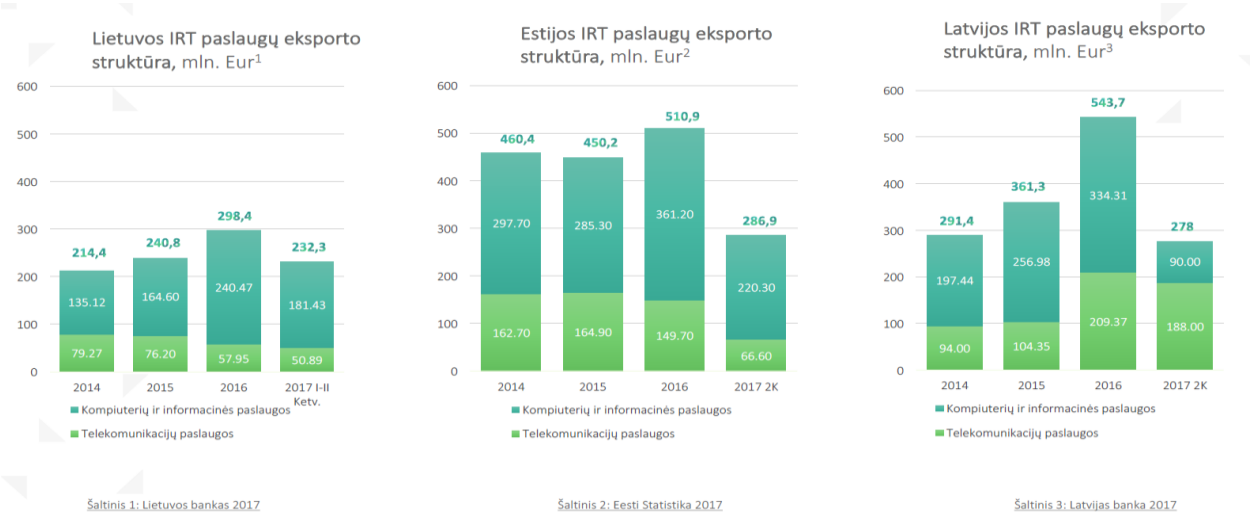




Šaltinis: Eurostat, 2016

[19] https://ec.europa.eu/digital-single-market/en/desi

[20] http://www.bdforum.org/wp-content/uploads/2017/11/2017_StateOfDigital-v3-004.pdf



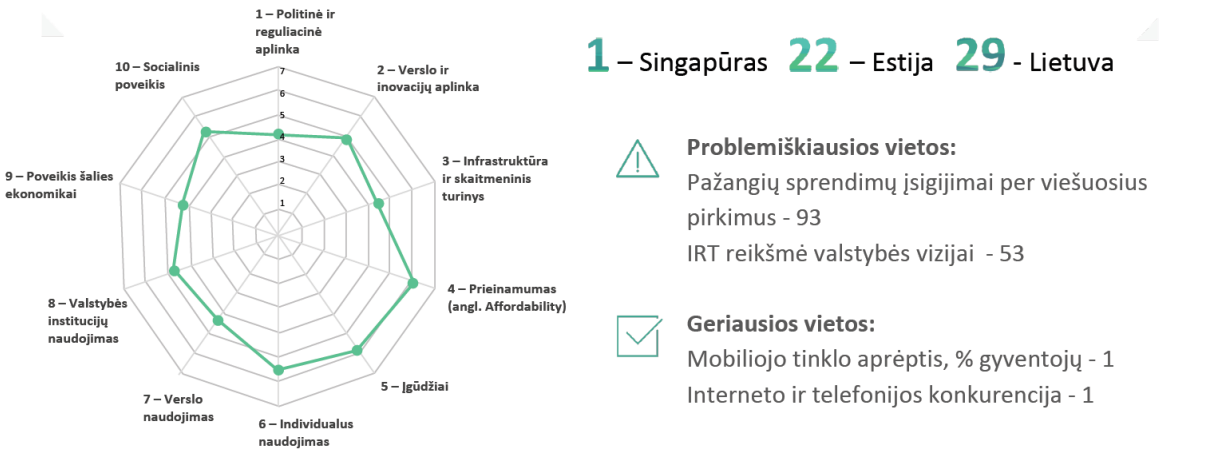
Šaltinis 1: Lietuvos bankas 2017

Šaltinis 2: Eesti Statistika 2017

Šaltinis 3: Latvijas banka 2017

(14) Turint galvoje, kad bent jau rašytiniais dokumentais Lietuva siekia tapti aukštųjų technologijų šalimi, ypač IRT technologijų šalimi, toks Lietuvos skaitmeninės ekonomikos atsilikimas net nuo savo artimiausių kaimynių, verčia susimastyti. Ypač apie tai, kaip Lietuva ketina auginti savo IRT sektoriaus konkurencingumą įtvirtindama KAM siūlomas valstybines monopolijas ir išstumdama privatų verslą iš paslaugų teikimo viešajam sektoriui.

(15) Kad valstybinių monopolijų egzistavimas neturi didelių šansų sustiprinti Lietuvos IRT sektoriaus konkurencingumo labai gerai iliustruoja *World Economic Forum* skelbiama pasaulinė informacinių technologijų ataskaita[21]. Analizuojant šioje ataskaitoje skelbiamus duomenis apie Lietuvos IRT sektorių tampa akivaizdu, kad IRT sektoriaus tarptautinius reitingus mažina būtent tie parametrai, kurie yra priskiriami valstybės atsakomybės sričiai – IRT sektoriaus vystymo vizijos neturėjimas ir nesugebėjimas įsigyti pažangių IRT sprendimų vykdant viešuosius pirkimus. Kai tuo tarpu IRT sektoriaus dalys, kuriuose veikia konkurencija yra išskiriamos kaip pažangiausios.



(16) Šių IRT sektoriaus statistinių duomenų kontekste nesunku suprasti, kad Lietuvos skaitmeninės ekonomikos rodikliai jau dabar kelia pakankamai didelį susirūpinimą. Net jeigu atskiri Lietuvos statistiniai rodikliai

[21] http://reports.weforum.org/global-information-technology-report-2016/economies/#indexId=NRI&economy=LTU

gerėja, globali skaitmeninė ekonomika vystosi gerokai greičiau ir Lietuva praranda bet kokį IRT sektoriaus pranašumą, kurį turėjo anksčiau.

(17) Savo ruožtu, sukurdama KAM siūlomas valstybės monopolijas Duomenų centrų paslaugoms ir Duomenų perdavimo paslaugoms Lietuva padidins savo IRT sektoriaus atsilikimą, sumažins savo verslo konkurencingumą pasaulinėje rinkoje ir IRT paslaugų eksportą, dar labiau paskatins aukštą pridėtinę vertą kuriančių IRT specialistų emigraciją. O svarbiausia, – visai tai būtų daroma nesant jokios racionalios priežasties. Valstybės tikėjimas, kad monopolizuodama IRT paslaugų teikimą viešajam sektoriui valstybė sukurs aukštesnės kokybės / saugesnes paslaugas prieštarauja elementariems ekonomikos dėsniams teigiantiems, kad monopolistas neturi jokios paskatos tobulėti ir niekada nepasiūlo geriausios kokybės ir kainos prekių ir paslaugų.

II. NEIŠNAUDOTAS INOVATYVIŲ TECHNOLOGIJŲ POTENCIALAS NELEIDŽIA LIETUVAI ŽENGTI KARTU SU PASAULIO TECHNOLOGIJŲ ŠALIMIS LYDERĖMIS

A. Lietuvos sumanios specializacijos strategija įgyvendinama paviršutiniškai

(18) 2015 m. buvo patvirtinta Lietuvos sumanios specializacijos strategija („**Strategija**“), kuria Lietuva nustatė savo mokslinių tyrimų, eksperimentinės plėtros (MTEP) ir inovacijų prioritetus, atsižvelgdama į turimus ar galimus konkurencinius pranašumus. Ši strategija parengta siekiant kurti stiprią, konkurencingą ir išmanią ekonomiką, grįstą moksliniais tyrimais ir inovacijomis. Strategijoje vienu iš prioritetų yra įvardijamos IRT infrastruktūros, debesų kompiuterijos sprendimai ir paslaugos. Tarp jų, svarbiausiomis technologijomis nurodomos:

(i) Veiklos procesų ir taisyklių modeliavimo ir integravimo metodai ir technologijos;
(ii) Informacinių sistemų modernizavimo ir pokyčių valdymo technologijos;
(iii) Verslo ir viešojo sektoriaus valdymo procesų automatizavimo ir optimizavimo technologijos;
(iv) Duomenų virtualizavimo, debesų kompiuterijos, skaitmeninės medijos technologijos;
(v) E-paslaugų ir debesų kompiuterijos saugos technologijos;[22]

(19) Vertėtų pažymėti, jog Strategijos pamatinis tikslas yra valstybės ir verslo bendradarbiavimas siekiant kurti inovacijomis grįstas technologijas ir paslaugas, bei neatsilikti nuo pasaulinių šalių-lyderių, kurios sumanias technologijas diegia viešosiose paslaugose.

(20) Lietuvos pasiryžimas investuoti į skaitmenines technologijas, debesų kompiuterijos paslaugas ir kitas inovatyvias technologijas, deja, apsiriboja tik deklaratyviu dokumentu. 2018 m. paskelbta antroji ataskaita „Sumanios specializacijos įgyvendinimo stebėsena“ nurodo, kad:

> *„Debesų kompiuterijos prioritetas, kitaip nei pirmiau aprašytieji, nepasižymi ypatingu moksliniu bendradarbiavimu bei mokslinių rezultatų potencialu, tačiau išsiskiria dviem komponentais: santykinai dideliu tyrėjų skaičiumi įmonėse bei santykinai aukštomis įmonių MTEPI išlaidomis. Šiuo atveju galima daryti prielaidą, kad debesų kompiuterijos prioritetas MTEPI veiklas sutelkia išskirtinai verslo sektoriuje.“*[23]

(21) Matoma, kad valstybė ne tik nesiekia investuoti į MTEP inovatyviose srityse, dar daugiau yra atsiribojama nuo bendradarbiavimo su verslu šioje srityje. Tokia praktika stabdo valstybės augimą konkurencingoje ir

[22] http://sumani2020.lt/apie-sumania-speciaizacija/prioritetai
[23] http://sumani2020.lt/images/documents/ss/ss_ataskaita_2018.pdf

globalioje IRT rinkoje, nėra kuriamos naujos sumanios technologijos ar paslaugos, nėra ugdomi žmogiškieji gebėjimai.

(22) Svarbu pabrėžti ir tai, kad KAM deklaruojama nuostata, jog siūlomos monopolizuoti paslaugos bus teikiamos išimtinai tik valstybės institucijoms, nepaneigia valstybės (kaip viešųjų ir privačių subjektų visumos) poreikio kurti inovatyvias technologijas ir investuoti į tokių technologijų tyrimus, kūrimą ir plėtrą.

B. Neišnaudotas inovacijų potencialas varžo Lietuvos konkurencingumą ir ekonomikos augimą

(23) Žvelgiant į tarptautinę praktiką, matoma, kad dažnai šalys nesugeba išnaudoti inovatyvių technologijų dėl žemo investicijų lygmens ir nenoro / negebėjimo prisitaikyti prie jau sukurtų technologijų. Tokia situacija pastebima ir Lietuvoje. Pavyzdžiui, analizuojant galimybę valstybės lygmeniu naudoti debesų kompiuterijos paslaugas, yra svarbu pabrėžti pagrindinius šios paslaugos privalumus (i) viešąsias debesijos paslaugas valstybė gali išbandyti nedarydama ženklių ar nepamatuotai didelių investicijų, kadangi yra naudojama jau sukurta infrastruktūra ir (ii) pradėti naudoti viešąsias debesijos paslaugas valstybė gali naudodamasi jau pasaulyje sukurtais įrankiais, dėl to nėra reikalinga prarasti kelerius metus laiko.

(24) Lietuvos, kaip valstybės nenoras naudotis jau sukurtomis viešosiomis debesijos paslaugomis ne tik IRT bet ir kituose sektoriuose, kaip sveikata, energetika ar transportas, riboja inovacijų ir technologijų progresą. Debesijos paslaugų, kurios yra jau sukurtos ir lengvai pasiekiamos ir pritaikomos Lietuvos institucijose, naudojimo ribojimas ne tik žlugdo valstybės institucijų modernų funkcionavimą, bet ir varžo verslo konkurencingumo augimą.

(25) Infobalt įsitikinimu, valstybės institucijų ir strateginės reikšmės verslo sektorių bendradarbiavimas yra gyvybiškai svarbus ne tik šalies ekonominiam augimui bet ir strateginiams saugumo interesams užtikrinti. Stiprus, konkurencingas ir inovatyvus informacinių ryšių ir technologijų sektorius yra neatsiejamas valstybės kibernetinio saugumo garantas. Todėl siekis reikšmingą dalį IRT rinkos perimti iš verslo ir jas monopolizuoti, ne tik pažeidžia konkurencijos laisvę (yra neteisėtas), stabdo Lietuvos inovacijų vystymąsi bet ir kelia grėsmę valstybei teikiamų paslaugų kokybei. Lietuvos atveju yra gyvybiškai svarbu valstybei skatinti IRT rinkos plėtrą iš rinkos reikalaujant aukštos kokybės ir standartų paslaugų bei produktų, todėl ketinimai pašalinti verslą iš duomenų centrų ir tinklo paslaugų tiekėjų sumažins Lietuvos IRT sektoriaus ekonominį potencialą ir pakenks nacionalinių IRT saugumo gebėjimų vystymuisi.

Priedas Nr. 3

PASAULINĖS PRAKTIKOS ANALIZĖ RODO, KAD DUOMENŲ SAUGUMAS NĖRA KURIAMAS MONOPOLIZUOJANT IRT PASLAUGŲ TEIKIMĄ

A. NATO skatina partnerystę su verslu naudojant debesų kompiuterijos paslaugas

(1) 2016 m. sausį NATO patvirtino Debesų kompiuterijos politiką (AC/322-D(2016)0001), kurioje nustatomos taisyklės ir reikalavimai debesų kompiuterijos paslaugoms. Šio dokumento tikslas yra įgalinti NATO naudotis bendra jau sukurta infrastruktūra ir geriausiomis pasaulinėmis technologijų praktikomis. Debesų kompiuterijos politika nustato bendrus, į paslaugas orientuotus debesų kompiuterijos infrastruktūros kūrimo, naudojimo ir dalijimosi principus, kurie leidžia pasiekti lengvesnį duomenų ir paslaugų prieinamumą, saugumą ir mobilumą.

(2) Patvirtinta debesų kompiuterijos politika numato, kad tik NATO konfidenciali informacija turi būti laikoma privačioje debesijos duomenų bazėje, kuri būtų valdoma pačios NATO arba aljanso valstybės narės. Tuo tarpu, visa kita, NATO riboto naudojimo informacija ir žemesnio saugumo lygio informacija (kuri sudaro apie 70-80% visos informacijos) yra laikoma viešose arba hibridinėse debesijos duomenų bazėse.

(3) NATO jau dabar laiko didžiąją dalį savo duomenų viešuose / hibridiniuose „debesyse“, pavyzdžiui duomenis, kurie neturi specifinės saugumo klasifikacijos. Toks vieno didžiausių pasaulyje valstybių aljanso siekis bendradarbiauti su verslu, naudojantis geriausiomis jau sukurtomis technologijomis, rodo organizacijos pasitikėjimą tarptautinėmis, ilgametę patirti IRT sektoriuje turinčiomis kompanijomis. NATO, išnaudodama jau sukurtas technologijas, išlieka inovatyvi ir progresyvi organizacija, kurios pavyzdžiu turėtų sekti ir Lietuva.

B. Latvija ir Estija renkasi bendradarbiavimą su verslu

(4) Kaimyninės valstybės yra pasitvirtinusios valstybės informacinių išteklių tvarkymo ir naudojimosi politikas. Skirtingai, nei Lietuva, mūsų kaimyninės valstybės siekia užtikrinti valstybės duomenų saugumą neeliminuodama verslo iš IRT paslaugų teikėjų ir siekia, kad tik ypatingos svarbos duomenys būtų tvarkomi išimtinai nacionalinių vyriausybių. Kiti svarbūs valstybiniai duomenys yra laikomi duomenų centruose, kurie įrengti pasitelkiant privatų verslą, valstybei nustačius aiškius saugumo kriterijus. Tokia valstybės politika skatina verslo inovacijų plėtrą ir kompetencijų privačiame sektoriuje augimą. Bendras valstybės ir verslo darbas leidžia užtikrinti aukščiausius saugumo reikalavimus valstybės duomenims ir ryšių perdavimo tinklams.

(5) Valstybės bendradarbiaudamos su inovatyviomis, dažnai ilgalaikę tarptautinę patirtį turinčiomis kompanijomis, gali užsitikrinti ne tik aukščiausios kokybės ir saugumo paslaugas, bet ir efektyviai išnaudoti patiriamus kaštus. Valstybės sąnaudos, patiriamos perkant IRT paslaugas iš privataus sektoriaus yra nepalyginamai mažesnės, nei tos, kurios būtų reikalingos pirkti paslaugas iš valstybinio IRT paslaugų teikėjo. Valstybinė įmonė ar institucija, kurios vienintelė veikla yra konkrečios paslaugos teikimas, atsižvelgiant į reikalingas investicijas, žmogiškuosius išteklius ir kitus aspektus, neturi galimybių pasiūlyti paslaugos už konkurencingą rinkos kainą.

2016 m. Latvijos Vyriausybė ir IT asociacija pasirašė bendradarbiavimo memorandumą, įtvirtinanti Latvijos siekį tapti Duomenimis grindžiama tauta (angl. Data Driven Nation). Pagrindiniai memorandumo tikslai – stiprinti Latvijos IRT rinką ir eksportą, išnaudoti verslo teikiamas galimybes stiprinant Latvijos

nacionalinę ekonomiką, pasiekti pilną skaitmeninės vyriausybės potencialą pagal modernios visuomenės ir ekonomikos reikalavimus bei didinti Latvijos ir jos ekonomikos konkurencingumą. Estijoje viešųjų debesijos paslaugų gairės numato duomenų tvarkymą pagal skirtingas duomenų kategorijas. Gairės reikalauja, kad ypatingos svarbos duomenys būtų laikomi Estijos teritorijoje, o visi kiti duomenys turi būti laikomi ES teritorijoje. Tokia Duomenų Centrų / Debesijos paslaugų politika leidžia verslui teikti IRT paslaugas valstybei, o valstybė savo ruoštu užsitikrina aukščiausius gaunamų paslaugų saugumo standartus.

Duomenų Centrų/ Debesijos paslaugų politika	
Latvija	Šiuo metu baigiamos derinti gairės, nustatančios debesijos paslaugų naudojimą viešajame administravime numato: • Duomenys, kurie turi „valstybės paslapties“ žymą yra laikomi valstybės kontroliuojamame Duomenų centre. • Ribotos prieigos informacija (duomenys oficialiam naudojimui, specialiems atvejams, verslo paslaptį saugantys duomenys, piliečių duomenys) yra laikoma valstybės ir privačiuose duomenų centruose, kurie atitinka specialius reikalavimus. • Kiti duomenys laikomi laisvai pasirenkamuose duomenų centruose.
Estija	Viešųjų debesijos paslaugų gairės numato duomenų tvarkymą pagal duomenų kategorijas: • Ypatingos svarbos duomenys (S3 klasifikacija) laikomi Estijos teritorijoje. • Visi kiti duomenys, įskaitant tam tikras grupes ribotos prieigos duomenų gali būti laikomi ES teritorijoje (pasitelkiant viešųjų debesijos paslaugų teikėjus) (S0 – viešai prieinami duomenys, S1 – duomenys tik vidiniam naudojimui, S2 – ribotos prieigos duomenys, su kuriais dirba tik teisėtą interesą turintys asmenys).